Transportation Security: Issues for the 112th Congress

David Randall Peterman
Analyst in Transportation Policy

Bart Elias
Specialist in Aviation Policy

John Frittelli
Specialist in Transportation Policy

February 1, 2011

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. The 110th Congress passed legislation to extend the existing authorization of such sums as may be necessary for TSA's aviation security functions through FY2011 (see P.L. 110-53, section 1618). Reauthorization of TSA functions may be considered in the broader context of a Department of Homeland Security reauthorization bill during the 112th Congress. Issues likely to arise include deployment of new checkpoint screening technologies; passenger screening procedures; implementation of the Secure Flight system to check passenger data against the consolidated terrorist database; air cargo security measures; and strengthening security of general aviation aircraft and airports.

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. In 2010, Congress expressed concern about the slow rate at which federal funds for transit and rail security were being expended. If the 112th Congress revisits the issue, it may consider the effectiveness of rail and transit security efforts to date, the potential for meaningful security improvement in this area, and its importance relative to other federal priorities.

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 is unlikely to be met, as foreign countries object to the costs of this screening and are dubious of the benefits. If Congress considers maritime security, it may examine the usefulness of this mandate, as well as the threat posed by the many small craft that populate commercial port areas and progress toward establishing harbor interagency operational centers.

Contents

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 this report 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]

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. The act gave TSA broad authority to assess vulnerabilities in aviation security and take steps to mitigate these risks. TSA's role in aviation security has been the subject of considerable congressional oversight. Particular issues of interest include

- progress toward meeting the statutory mandate to screen all cargo placed on passenger airplanes, particularly inbound international shipments;

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

- options for screening and securing shipments placed on all-cargo aircraft;
- deployment of new checkpoint screening technologies and associated changes in passenger screening procedures;
- options for privatizing airport screening operations;
- implementation of the Secure Flight system to check passenger data against the consolidated terrorist database; and
- options for strengthening security of large general aviation aircraft.

Congress passed legislation in the 110th Congress extending authorization of such sums as may be necessary for TSA aviation security functions through FY2011 (see the Implementing the 9/11 Commission Recommendations Act of 2007, P.L. 110-53, section 1618). As this authorization is set to expire, aviation security issues may be examined during the first session of the 112th Congress, probably in the context of a multiyear TSA reauthorization measure.

A Risk-Based, Multi-Layered Approach

Aviation security policy since September 11, 2001, has consisted of two basic principles: a risk-based approach for allocating limited security resources to where they are considered most needed, and a multi-layered strategy that establishes redundancies to thwart a potential terrorist attack.

The risk-based approach implemented by TSA has been criticized for overemphasizing the screening of airline passengers rather than focusing on threats in other areas—namely, air cargo operations; airport access controls; protecting airliners from shoulder-fired missiles; and the security of general aviation aircraft. In essence, these critics argue that the implementation of aviation security policy since September 11, 2001, has focused too heavily on protecting aircraft from past attack scenarios—such as suicide hijackings and luggage bombs carried out by airline passengers—and has not given enough attention to other potential vulnerabilities.

Given the emphasis on protecting against bombings and suicide hijackings, the multi-layered concept for aviation security is most apparent in the protection of passenger airliners. Passengers undergo prescreening to check their names against lists of known and suspected terrorists, then passengers and their carry-on items are screened and checked baggage is passed through explosive detection systems (EDS) prior to aircraft boarding. Once onboard, security measures such as air marshals, hardened cockpit doors, and armed pilots provide added layers of security to thwart an attempted hijacking. The effectiveness of TSA's implementation of virtually all of these security layers has been brought into question at one time or another since its creation.

Passenger Prescreening

Efforts to improve passenger prescreening have been affected by concerns over the adequacy of measures to protect fliers' personal information and not infringe upon their civil rights. Critics have argued that TSA's ever-expanding vision for prescreening was to include data mining of commercial and government databases to look for indicators that someone may pose a threat, and searches of notoriously inaccurate criminal databases. These concerns were spurred by vague statements issued by TSA as to how it might authenticate passenger identity and check for possible links to terrorism along with media reports linking passenger prescreening to

controversial proposals such as the Department of Defense's Total Information Awareness program to detect terrorists by mining personal data. This controversy ultimately led TSA to scrap its proposed enhanced passenger prescreening system, the Computer Assisted Passenger Prescreening II (CAPPS II), in August 2004, and pursue enhanced prescreening capabilities under a new system called Secure Flight. While Secure Flight is touted to be a significantly scaled down approach to prescreening compared to CAPPS II, concerns over data protections and redress procedures for passengers falsely identified by the system significantly delayed its deployment.

TSA has addressed various concerns over traveler privacy, data retention, and reducing false positives. On October 28, 2008, it published a final rule detailing the planned operational implementation of Secure Flight.[2] Under this regulation, TSA has phased in use of the Secure Flight system to check passenger records against the consolidated terrorist database for domestic flights and, subsequently, for international arrivals and departures. As of November 30, 2010, TSA indicated that 100% of domestic and international passenger flights were being checked under its Secure Flight protocols. However, TSA currently does not perform Secure Flight checks for all overflights that cross through U.S.-controlled airspace but do not land at a U.S. destination. Watchlist checks of overflights remain an objective pending resolution of various international agreements. TSA took over responsibility for passenger checks of inbound international arrivals from U.S. Customs and Border Protection, but overflights would represent a new category of covered operations encompassing some airlines that do not serve the United States.

Provisions in P.L. 110-53 also required the Department of Homeland Security (DHS) to establish appeals procedures for passengers misidentified though prescreening processes and establish an Office of Appeals and Redress charged with implementing a "timely and fair process" for airline passengers delayed or denied boarding due to suspected misidentifications. DHS has addressed this mandate by establishing the Travel Redress Inquiry Program (DHS TRIP). DHS TRIP allows passengers seeking redress, or their designated representatives, to file complaints using either an online system or by completing and mailing a form. With the Secure Flight system now in place, the timeliness and effectiveness of handling and resolving complaints received through DHS TRIP may be a particular issue of interest for congressional oversight during the 112th Congress.

TSA had also implemented a Registered Traveler (RT) program that was intended to expedite checkpoint screening of frequent fliers who voluntarily submit background information and biometric identifiers. While TSA had approved RT programs operated by multiple vendors at several airports nationwide, it was left up to airport operators to determine if they wished to participate. The airline industry, which once backed this program as a means to reduce hassles for frequent fliers, came to view the manner in which it was implemented as having limited and questionable benefits. Airlines have instead pressed for express lanes for their best customers, including frequent fliers and first class travelers. Also, the use of the RT program as a testbed for streamlined screening technologies and procedures failed to yield demonstrable benefits.

Because of these perceived shortcomings, coupled with business failures among RT providers, the initial RT program was halted. While there has been some effort to revamp the RT program, TSA and industry partners have continually struggled to define the program's objectives and implementation. Language in the House-passed TSA Authorization Act considered during the 111th Congress (H.R. 2200) sought to revamp the RT program by reinstating security threat

[2] U.S. Department of Homeland Security, Transportation Security Administration, "Secure Flight Program: Final Rule," 72 *Federal Register* 64018-64066, October 28, 2008.

assessments as an integral component, allowing RT providers to conduct private background checks, and implementing alternative screening procedures for RT members who hold top secret government security clearances. The bill also would have required TSA to develop a known traveler credential incorporating biometric data for individuals with government security clearances including members of the armed services, flight crew certified by the Federal Aviation Administration (FAA), and law enforcement personnel, and to establish procedures allowing such individuals to bypass screening checkpoints. Options for making an RT program an effective component of aviation security may be an area of specific interest for the 112th Congress.

Passenger Screening[3]

The 9/11 Commission recommended that TSA give priority attention to implementing technology and procedures for screening passengers and baggage for explosives. This need has been highlighted by several unsuccessful terrorist acts, including the December 2001 shoe bombing attempt, the foiled plot to bomb U.S.-bound airliners using liquid explosives uncovered in August 2006, and the attempted bombing of Detroit-bound passenger airliner on December 25, 2009.

During 2010, TSA introduced whole body imaging (WBI) systems at airport checkpoints around the United States. These systems, which TSA refers to as advanced imaging technology (AIT), capture an image of what lies underneath an individual's clothing using one of two technologies: X-ray backscatter and millimeter wave imaging. The technologies do not specifically identify explosives, but can reveal concealed items that would not be detected by walkthrough metal detectors, including explosives and non-metallic weapons. Polling data indicate that about 75%-80% of Americans support the use of AIT at airport checkpoints.[4] However, AIT has met with objections from groups such as the American Civil Liberties Union, which has urged Congress to ban the use of whole body imaging technologies as a method for primary screening.[5] To allay some of these concerns, millimeter wave systems used by TSA apply privacy filters that may blur facial features and sensitive areas. X-ray backscatter systems currently deployed use computer algorithms to render a "chalk outline" sketch of the individual and discernible concealed items. There are also concerns about potential human health effects of X-ray backscatter screening, although TSA contends that the levels of ionizing radiation emitted by approved backscatter systems are well below levels considered safe for human exposure.

Passengers who object to WBI screening may opt instead for pat-down searches. However, in 2010, pat-down procedures were modified and made more invasive. Additionally, TSA may require a pat-down if a passenger sets off a walkthrough metal detector alarm or if a WBI image arouses suspicion. Under current TSA procedures, an individual selected for WBI or a pat-down must undergo that process, and may not choose to be screened by a walkthrough metal detector or to exit the screening process and not fly. This situation poses a dilemma for individuals uncomfortable with both WBI screening and pat-down searches.

---

[3] For further reading on this topic see CRS Report R41502, *Changes in Airport Passenger Screening Technologies and Procedures: Frequently Asked Questions*, by Bart Elias, and CRS Report R40543, *Airport Passenger Screening: Background and Issues for Congress*, by Bart Elias.

[4] See AIT polls at http://www.tsa.gov/approach/tech/ait/reading.shtm.

[5] Statement of Timothy D. Sparapani, ACLU Legislative Counsel, Before the Senate Committee on Commerce, Science, and Technology, Regarding the U.S. Transportation Security Administration's Physical Screening of Airline Passengers and Related Cargo Screening, April 4, 2006.

TSA also has been deploying advanced technology X-ray equipment capable of providing multiple view angles and automated threat detection capabilities to aid in screening carry-on items and handheld bottled liquids scanners to screen for liquid explosives. During the 112th Congress, TSA's investment and deployment strategies for these technologies is likely to be an issue of considerable interest.

The use of AIT in particular was addressed in legislation considered during the 111th Congress. A provision in the House-passed TSA Authorization Act (H.R. 2200) would have prevented TSA from using WBI systems during routine, primary passenger screening, and would have required that TSA offer pat-down searches as an alternative to WBI scans for any passengers selected for secondary screening. The bill would also have prevented TSA from storing, transferring, sharing, or copying any WBI images once a passenger is cleared for boarding, and would require TSA to make available information regarding the technology and related privacy policies to any passenger selected to undergo WBI screening. In contrast, Senator Bennett offered the Securing Aircraft From Explosives Responsibly: Advanced Imaging Recognition (SAFER AIR) Act of 2010 (S. 3536, 111th Congress), which called for the expeditious deployment of AIT and other advanced screening technologies for primary screening of aircraft passengers. It too included provisions to protect privacy, many of which parallel current TSA practices. Representative Paul introduced the American Traveler Dignity Act of 2010 (H.R. 6416, 111th Congress), which would have barred TSA, TSA screeners, private airport security screeners, or others involved in the screening process from claiming immunity from prosecution in a criminal or civil proceeding arising as the result of whole-body screening or a pat-down search.

Passenger checkpoint efficiency has also been an issue. TSA has struggled to strike a balance between effectively screening passengers and avoiding undue delays and hassles to travelers. While passenger wait times at smaller airports are usually less than the stated objective of 10 minutes, average wait times at major airports are typically greater.

Further, audits have concluded that screener performance needs improvement. The DHS Office of Inspector General found that screener training, screening technology, policies and procedures, and management and supervision of screening operations all contributed to observed deficiencies in performance. Covert testing by the Government Accountability Office (GAO) found deficiencies in detecting improvised explosives and incendiary devices concealed on passengers and in their carry-on items, despite stepped-up secondary screening for explosives.[6] In December 2010, media reports revealed that a man with a loaded pistol in his carry-on bag passed through airport security undetected and boarded an international flight at Houston Bush Intercontinental Airport. The incident renewed concerns over the capability of screeners to detect potential threats.[7]

Federalization and Privatization of Airport Screening

As it debated aviation security immediately following September 11, 2001, Congress considered whether airport security screening should be conducted by federal employees. At that time,

[6] U.S. Government Accountability Office, *Aviation Security: Vulnerabilities Exposed Through Covert Testing of TSA's Passenger Screening Process*, Statement of Gregory D. Kutz, Managing Director, Forensic Audits and Special Investigations, and John W. Cooney, Forensic Audits and Special Investigations Before the Committee on Oversight and Government Reform, House of Representatives, November 15, 2007.

[7] Matthew Mosk, Angela Hill, and Timothy Fleming, "Gaping Holes in Airline Security: Loaded Gun Slips Past TSA Screeners," *ABC News*, December 16, 2010.

screening operations suffered from high turnover, poor supervision and training, low wages, and a lack of regulatory oversight. Federalizing the screener workforce was intended to address these deficiencies. However, while Congress ultimately resolved to federalize the screener workforce at most airports, ATSA also set up a pilot program using contract screeners at five airports and gave all airports the option to request private screeners starting November 19, 2004. Most airports have shown little interest in this option. Some airports may have liability concerns, although language in the FY2006 Homeland Security Appropriations Act (P.L. 109-90, section 547) indemnifies airports from liability relating to their decisions to use either private or federal screeners and to claims of negligence or intentional wrongdoing on the part of screeners, whether federal or private employees. Few airports have been fully converted to private screening operations, and in January 2010 TSA announced that it would not further expand the program. However, renewed congressional interest in expanding private screening suggests that this could be a significant issue in the 112th Congress.

Baggage Screening

While airports are, for the most part, meeting mandated requirements to inspect all checked bags with explosive detection system (EDS) equipment, they are struggling to integrate these systems into baggage handling and sorting facilities. To address these needs, Congress established (in Vision 100, P.L. 108-176) an Aviation Security Capital Fund with a mandatory funding level of $250 million annually and a total authorized funding level of $500 million per year through FY2007. Provisions to expedite and increase funding for in-line baggage screening were included in the Intelligence Reform and Terrorism Prevention Act (P.L. 108-458). However, meeting funding needs for airport security projects and setting priorities amid budgetary constraints remain ongoing challenges. Provisions in P.L. 110-53 extended the authority for mandatory funding of the Aviation Security Capital Fund through 2028, and authorized increased discretionary funding level of $450 million annually for FY2008 through FY2011 for in-line baggage screening. The act also required TSA to prioritize airport projects based on risks and other considerations. Improvement of baggage screening systems remains as a major aviation security issue for the 112th Congress.

Over $650 million of American Recovery and Reinvestment Act (ARRA; P.L. 111-5) funding for aviation security was designated for checked baggage screening projects. Additionally, $778 million was appropriated in FY2010 for EDS and explosives trace detection (ETD) systems acquisition and installation. Despite these appropriations, TSA still faces outlays for replacing explosives detection systems purchased a decade ago that are now nearing the end of their expected service lives, while keeping maintenance costs in check and preparing to handle larger passenger flows in the future. TSA must balance funding of new screening facilities with payment to airports that have already completed projects with their own funds under TSA letters of intent promising reimbursement. TSA authorization legislation passed by the House during the 111th Congress would have required TSA to establish a process for resolving reimbursement claims for airports that have incurred eligible costs associated with the construction of in-line baggage screening systems.

Air Cargo Security[8]

The October 2010 discovery of two explosive devices being prepared for loading on overseas U.S.-bound all-cargo aircraft renewed policy debate over air cargo security measures and prompted some policymakers to call for comprehensive screening of all air cargo, including shipments that travel on all-cargo aircraft. U.S. policies and strategies for protecting air cargo have focused on two main perceived threats: the bombing of a passenger airliner carrying cargo and the hijacking of a large all-cargo aircraft for use as a weapon to attack a ground target. The October 2010 incidents highlighted the potential threat of explosives in the all-cargo sector.

The Implementing the 9/11 Commission Recommendations Act of 2007 (P.L. 110-53, section 1602) required the screening of all air cargo placed on passenger aircraft by August 2010, using methods such as X-ray systems, explosives detection systems, explosives trace detection, TSA-certified canine teams, or physical searches with manifest verification, in a manner that provides a level of security equivalent to the screening of passenger-checked baggage. These mandates were opposed by various stakeholders in the air cargo industry who regard these requirements as overly burdensome and costly.[9]

TSA has addressed air cargo in the context of supply chains, by delegating authorized screeners to examine cargo at Certified Cargo Screening Program facilities, such as factories and consolidation points, coupled with additional measures to insure the security and integrity of freight screened at off-airport facilities. While TSA maintains that this approach meets the requirements of the legislation, some Members of Congress have argued that the intent of the legislation was for TSA to play a more direct role in overseeing screening and for screening to occur in closer physical proximity to airports. The House-passed TSA authorization bill considered during the 111th Congress would have required TSA to report on the status of the Certified Cargo Screening Program. A separate provision would have required TSA to increase the number of canine teams used for air cargo screening. The bill also would have directed TSA to establish an air cargo working group, as part of the Aviation Security Advisory Committee (ASAC), to address air cargo security issues.

Inbound international cargo poses a particular challenge for TSA. While all cargo traveling on domestic passenger flights is now being screened, full compliance for inbound international flights may not be achieved until August 2013. A provision in the TSA authorization bill passed by the House during the 111th Congress would have required the DHS to establish a system to verify that all inbound international air cargo placed on passenger aircraft be screened for explosives within two years of enactment. The bill also called for a GAO study of inbound air cargo screening and quarterly audits detailing the percentage of and rationale for inbound international air cargo being exempted from screening requirements.

Following the October 2010 incidents, there has been considerable interest in increasing international cooperation with respect to air cargo security, screening, and inspection methods. TSA has entered into agreements with the European Union, Canada, and Australia, and is working with the International Civil Aviation Organization (ICAO) to draft worldwide standards for air cargo security. Nonetheless, TSA has limited resources and limited authority to oversee the

[8] For further reading on this topic see CRS Report R41515, *Screening and Securing Air Cargo: Background and Issues for Congress*, by Bart Elias.

[9] "House To Consider Bill Today Requiring Additional Cargo Screening," *Transportation Weekly*, Jan. 9, 2007, p. 7.

security of international air cargo shipments bound for the United States. Consequently, efforts to improve international cooperation and strengthen TSA's role in monitoring air cargo security practices outside the United States are likely to be of particular interest to the 112th Congress.

On November 16, 2010, Representative Markey introduced the Air Cargo Security Act (H.R. 6410, 111th Congress) to require screening of all cargo transported on all-cargo aircraft, including U.S.-bound international shipments, in a manner commensurate with the screening requirements for passenger checked baggage. The legislation also includes provisions requiring inspections of foreign air cargo shipping facilities that handle U.S.-bound flights and formal security training programs for cargo handlers. On November 17, 2010, Senator Casey introduced a similar measure (S. 3954, 111th Congress) in the Senate.

Congress has also considered ways to mitigate the effects of an explosive device concealed in air cargo or in hold baggage. The 9/11 Commission recommended deploying at least one hardened cargo container on each passenger airliner for carrying suspect cargo. P.L. 110-53 contains a provision that required the DHS to complete an evaluation of its hardened cargo container pilot program and, based on this evaluation, to carry out a risk-based deployment of hardened cargo containers for use on commercial flights. Under this provision, the cost of acquiring, maintaining, and replacing hardened cargo containers would be provided for by the DHS (see P.L. 110-53, section 1609). While the pilot program has been completed, no requirement has been imposed for operational deployment of hardened cargo containers.

TSA regulations require all-cargo operators to protect against unauthorized access to large all-cargo aircraft. Secured areas of airports have been expanded to include cargo operations areas. Regulations also impose requirements on freight forwarders that ship by air (referred to as indirect air carriers) and require background checks and security threat assessments for all workers with access to air cargo, including an estimated 51,000 off-airport employees of freight forwarding companies. TSA has established an industry-wide database of known shippers to allow freight forwarders and airlines to vet cargo shipments.

Airport and Aircraft Access Controls

While ATSA mandated background checks for all workers with unescorted access to passenger aircraft and secured areas of airports, in some cases airport workers are permitted to bypass screening checkpoints. Legislation introduced in the 108th Congress called for the physical screening of all workers with access to aircraft or secured areas. In FY2008 DHS appropriations (P.L. 110-161), funding was provided to TSA for a pilot program to assess physical screening of airport employees. Based on the results, TSA has implemented increased random and targeted screening of airport workers. However, airport workers do not routinely undergo security screening, except at a few airports like Miami and Orlando. P.L. 110-161 also established civil penalties for employers that fail to collect airport-issued security badges from employees whose airport jobs are terminated.

ATSA called for TSA to explore the use of biometrics and other identification technologies for transport workers and the use of biometrics for airport access controls. It is not anticipated that a common biometric identifier will be implemented across airports in the United States in a manner similar to the Transportation Worker Identification Card (TWIC) program for controlling access to seaports. However, the Terrorism Prevention Act (P.L. 108-458) required TSA to issue guidance on the use of biometrics for airport access controls and to verify the identity of law enforcement officers authorized to carry firearms on passenger airliners. P.L. 110-53 included

language requiring TSA to report on its progress implementing access control measures for airline crew members and requires TSA to establish a national registry and biometric access credential for law enforcement officers authorized to fly armed on commercial passenger aircraft (see sections 1614 and 1615). During the 111th Congress, a provision in the House-passed TSA authorization measure (H.R. 2200) would have directed TSA to carry out a demonstration program to assess the use of biometric identifier access systems for secure and sterile areas of airports. Many airport operators have expressed interest in the use of biometrics, but several have stated their reluctance to invest in biometric systems for access control because no standards or regulatory requirements have been established by TSA.

In-Flight Security Measures

Existing in-flight security measures consist primarily of federal air marshals, armed pilots, and hardened cockpit doors. The Federal Air Marshal Service was greatly expanded under ATSA and air marshals are required on all high-risk flights.

Airline pilots may receive training allowing them to serve as armed Federal Flight Deck Officers (FFDOs) under provisions set forth in the Homeland Security Act of 2002 (P.L. 107-296). Vision 100 (P.L. 108-176) expanded the program to include all-cargo pilots and other flight crew members such as flight engineers. Congress has maintained funding levels for both the FFDO program and cabin crew self-defense training at about $25 million annually. While the program has quietly added many armed pilots as an added layer to protect against hijackings, there are lingering concerns that the application procedures are too cumbersome and the training site is too remote to accommodate many pilots interested in participating.

ATSA also mandated the implementation of hardened cockpit doors and stringent controls regarding access to the flight deck. The Terrorism Prevention Act contained a provision to study the use of secondary flight deck barriers—a concept United Airlines initially pursued on its own initiative—to mitigate the vulnerability introduced when a hardened cockpit door is opened in flight for meal service or when a pilot needs to access the aircraft lavatory. Legislation introduced in the 110th Congress (see H.R. 3925, 110th Congress) sought to require the installation of secondary flight deck barriers for both air carrier aircraft that are equipped with hardened cockpit doors and also for air carrier aircraft without a hardened cockpit door, which includes many large cargo aircraft that are exempt from the requirements to install such doors.

Options for improving aircraft survivability in the event of bombings have also been discussed in Congress. P.L. 110-53 (section 1610) included a provision directing the DHS to expedite research and development of technologies to mitigate the introduction of an explosive device on a passenger airplane or reduce the damage such a device could cause on the ground or in flight. Along similar lines, the FAA has issued proposed rulemaking for security considerations in the design of large jet airliners, including improving systems survivability, cockpit and cabin fire suppression, improving flight deck barriers, and creating areas onboard where explosives discovered during flight can be contained to mitigate damage caused by a detonation.[10]

[10] Federal Aviation Administration, "Security Related Considerations in the Design and Operation of Transport Category Airplanes; Proposed Rule," 72 *Federal Register*, 629-639, January 5, 2007.

The Shoulder-Fired Missile Threat

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, brought into the public policy spotlight by the November 2002 attempted shoot-down of 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."[11] Since then, Department of State and military initiatives seeking voluntary reductions of man-portable air defense systems (MANPADS) stockpiles have reduced worldwide inventories by at least 30,000.[12] Despite this progress, many such weapons may not be accounted for. This threat, combined with the limited capability to improve security beyond airport perimeters or modify flight paths, leaves civil aircraft vulnerable, especially overseas in conflict zones and other high risk areas.

The most visible initiative to address the threat was the multiyear Counter-MANPADS (C-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 the high acquisition and life-cycle costs of these units. The units do not protect against the full range of potential missile threats to civil airliners, but do appear to provide effective protection against heat-seeking MANPADS. The airlines, which continue to face economic difficulties, have not voluntarily invested in these systems and argue that the costs 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, which comprises 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 escorts equipped with anti-missile technology, have been considered on a more limited basis, but these options appear likely to be of limited effectiveness.

At the airport level, improving security and reducing the vulnerability of flight paths to potential MANPADS attacks continue 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 obstacles because of limited resources and large geographic areas where aircraft are vulnerable to attack. 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.

General Aviation Security

Security measures for general aviation aircraft have been a particularly controversial subject. General aviation restrictions are most prevalent in the Washington, DC, area, where the city is encircled by a 15-mile radius flight restricted zone in which general aviation operations are significantly limited, and a larger air defense identification zone in which pilots must strictly adhere to special air traffic control procedures. In August 2005, the DHS implemented a security plan permitting certain general aviation flights—mostly large charter and corporate operations—

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

[12] Ibid.

to resume at Washington Reagan National Airport (DCA), which is located at the center of the flight restricted area. Operations at smaller general aviation airports located within the 15-mile flight restricted zone are highly restricted, requiring pilots to undergo background checks and strictly adhere to special airspace security procedures.

At various times, flight restrictions have also been put in place over New York City, Chicago, and elsewhere. General aviation pilots have been restricted from flying over certain theme parks and over stadiums during major sporting events, leading some general aviation advocates to question whether special interests were using the umbrella of security concerns to curtail unwanted advertising overflights. Restricted airspace violations have averaged more than 1,000 per year since the terrorist attacks of 2001, almost half of them around Washington, DC. The FAA reduced the size of the Washington air defense identification zone to a 30-mile ring in August 2007, but imposed speed restrictions within that ring, as well as inside a larger 60-mile ring below 18,000 feet. Most small general aviation aircraft are not affected by these speed restrictions, which are largely designed to aid in early detection of fast-moving aircraft that may pose threats.

About one-quarter of airspace violations have occurred in temporarily restricted airspace around sites during presidential visits. The scope of restricted airspace around sites visited by the President has been of particular concern to general aviation operators because the size of these areas has grown significantly, identifying the boundaries of these temporary restrictions is often difficult for pilots, and systems for disseminating information regarding the location and effective times of restrictions are imperfect.

Securing general aviation operations continues to be a significant challenge because of the diversity of operations, aircraft, and airports. Measures put in place thus far, such as the Airport Watch program and TSA's general aviation security guidelines, rely heavily on the vigilance of pilots to detect and report suspicious activity. Flight training providers are engaged in verifying citizenship or confirming that background checks have been properly completed by TSA before providing training to foreign nationals, as mandated under P.L. 108-176. The Terrorism Prevention Act allows aircraft leasing and charter companies to voluntarily provide TSA with names of prospective customers for prescreening against the consolidated terrorist watchlist. Also, the FY2006 DHS appropriations act (P.L. 109-90) required the DHS to assess security vulnerabilities from general aviation aircraft and identify steps that can be taken to enhance the security of general aviation aircraft and airports. A provision in P.L. 110-53 requires TSA to develop and implement a standardized risk assessment program at general aviation airports. The law also requires international general aviation flights to submit passenger information and advance flight notification to U.S. Customs and Border Protection prior to entering U.S. airspace.

In October 2008, TSA issued a proposal requiring adoption of security programs by general aviation reliever airports, which relieve congestion from major commercial airports, and general aviation airports that regularly serve scheduled commuter and public charter flights.[13] Under the proposal, these airports would be required to designate an airport security coordinator, establish procedures for law enforcement support and incident management, implement training programs for law enforcement personnel assigned to the airport, establish procedures for informing the

[13] Department of Homeland Security, Transportation Security Administration. "Large Aircraft Security Program, Other Aircraft Operator Security Program, and Airport Operator Security Program; Proposed Rule." *Federal Register, 73*(211), October 30, 2008, 64790-64855.

public regarding airport security matters, and establish systems for maintaining security-related records of law enforcement response to incidents that occur at the airport.

TSA also proposed to implement a variety of security measures for operators of all general aviation aircraft weighing more than 12,500 pounds, including privately owned, fractionally owned, and corporate aircraft.[14] These measures were to include fingerprint-based criminal history records checks for all flight crew members; terrorist watch-list checks of all passengers; security inspections of aircraft; and biannual security compliance audits. In addition, operators of all aircraft weighing more than 45,500 kilograms (roughly 100,000 pounds) would have been required to screen passengers and their accessible property. Similar security measures are already required for charter operators. After airports and operators of large aircraft objected to the burden that would be imposed on general aviation operations that were not previously subject to security-related regulations, congressional interest led TSA to revise its proposal, weighing risk factors and associated costs and benefits. The House-passed TSA authorization bill in the 111th Congress would have required TSA to establish a general aviation security working group to address security issues affecting general aviation. TSA is expected to release a revised regulatory proposal for general aviation operations in 2011. This may be an issue of particular interest to the 112th Congress, given the extensive controversy surrounding the 2008 notice of proposed rulemaking.

Transit and Passenger Rail Security[15]

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. 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 can be taken 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.

[14] Ibid.

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

On May 21, 2007 DHS announced completion of a transportation sector-specific plan (along with the other sector plans) and transportation mode-specific annexes, identifying critical assets, evaluating the risk to them, and developing measures to protect them. GAO noted that "these plans are only a first step ... [they] are not required to address how the sector is actually assessing risk and protecting its most critical assets."[16]

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. These included authorizing $3.5 billion for FY2008-FY2011 for grants for public transportation security, with $840 million for security-related operating expenses and $100 million for research and development (sections 1406 and 1409); $2 billion for grants for railroad security (section 1513), including $200 million for safety improvements to rail tunnels in New York, Baltimore, and Washington (section 1515), and $132 million for research and development (section 1518); and $95 million for grants for over-the-road bus security (sections 1532 and 1535). Public transportation agencies and railroads considered to be high-risk targets by DHS are required to have security plans approved by DHS (sections 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 (sections 1414 and 1522), and gave DHS the authority to regulate rail and transit employee security training standards (sections 1408 and 1517).

In a 2009 report, GAO contended: "TSA should conduct a risk assessment for the mass transit and passenger rail systems that combines the results of threat, vulnerability, and consequence assessments. Until the overall risk to the entire system is identified through such an assessment, TSA cannot best determine how and where to target its limited resources to achieve the greatest security."[17]

The Department of Homeland Security provides grants for transit, passenger rail, and freight rail security under the Urbanized Areas Security Initiative program. Congress provided $150 million for these grants for FY2005 and again for FY2006, $275 million for FY2007, $400 million for FY2008 and again for FY2009, and $300 million for FY2010. In 2009 Congress noted that, according to DHS, about 90% of the FY2006 funding for transit and rail security had not yet been expended;[18] in 2010, appropriators reiterated their concern about the slow pace of spending of transit and rail security grant funds.[19]

[16] Government Accountability Office, *Critical Infrastructure: Challenges Remain in Protecting Key Sectors*, GAO-07-626T, March 20, 2007, p. 5.

[17] Government Accountability Office, *Transportation Security: Keys Actions Have Been Taken to Enhance Mass Transit and Passenger Rail Security, But Opportunities Exist to Strengthen Federal Strategy and Programs*, GAO-09-678, June 24, 2009, p. 58.

[18] H.Rept. 111-298, Conference report to accompany H.R. 2892, the Department of Homeland Security Appropriations Act, 2010, p. 107.

[19] Senate Committee on Appropriations, S.Rept. 111-222 on the Department of Homeland Security Appropriations Bill, 2011, p. 119.

Port and Maritime Security Issues[20]

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. The 112th Congress may wish to assess four current port security initiatives: the 100% container scanning requirement; the threat posed by small craft; harbor interagency operational centers; and 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 the 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 indicated that it intends to seek an extension to the 2012 deadline, citing numerous challenges to implementing the 100% scanning requirement at overseas ports.[21] DHS appears to favor pursuing 100% scanning at only selected overseas ports deemed high risk.[22]

Meeting the 2012 deadline is unlikely since 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.[23] Customs and Border Protection (CBP) has tested the feasibility of scanning all U.S. bound containers at several overseas ports.[24] In a report to Congress, CBP identified and explained numerous operational, technical, logistical, financial, and diplomatic obstacles encountered during these tests.[25] The report includes communications from host government officials explaining their objections to pursuing 100% container scanning.[26] Singapore decided not to participate in the test[27] and Japan has also raised objections to 100% scanning.[28]

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

[21] 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.

[22] 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.

[23] 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.

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

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

[26] Ibid, Appendix A.

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

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

Threat Posed by Small Craft

The use of smaller vessels by terrorists to smuggle weapons or themselves onto U.S. shores or to conduct suicide bombings against larger cargo or passenger ships, as they did to the Navy's *U.S.S. Cole* and to the French oil tanker *Limberg*, is a concern. There are too many smaller boats for the Coast Guard to track and recreational boaters oppose tracking because of the cost of transponders and concerns about privacy.[29] Even if small vessels were tracked, there is skepticism whether there would be sufficient time to thwart an attack since small vessels routinely sail next to potential targets in a busy harbor environment. Based on a DHS strategy report, it appears the Coast Guard has no immediate plans to require smaller vessels be outfitted with transponders but will continue to pursue methods to identify small craft.[30]

Harbor Operation Centers

Interagency Operation Centers (IOCs) were authorized in the Security and Accountability for Every Port Act of 2006 (P.L. 109-347, sec. 108). The U.S. Coast Guard is establishing IOCs in major U.S. ports where federal and local law enforcement agencies can share maritime intelligence and coordinate responses when the need arises, such as boarding higher risk vessels.[31] The Coast Guard is planning to co-locate these centers with existing Vessel Traffic Service stations where Coast Guard "watch-standers" track and monitor ship movements in a harbor for safety. While these command centers appear to be a means by which law enforcement agencies can "connect the dots" in the maritime environment, Congress has been concerned with the pace at which the Coast Guard is setting up these centers.

Transportation Worker Identification Credential

On January 25, 2007, TSA and the Coast Guard issued a final rule implementing the Transportation Worker Identification Credential (TWIC) at U.S. ports.[32] Longshoremen, port truck drivers, merchant mariners, and other workers entering a port must apply for a TWIC card to obtain unescorted access to port facilities or vessels. The card uses biometric technology for positive identification and 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. These standards examine criminal history, immigration status, mental capacity, and terrorist activity to determine whether a worker poses a security threat. A worker pays a fee of about $133 to cover the cost of administering the cards. Port facility operators will be responsible for deploying card readers at the gates to their facilities. TSA is testing card readers at a handful of ports to determine the best kind of card reader technology to require. Congress has been concerned with how the TWIC requirement has affected hiring practices and port and vessel operations.

---

[29] Statement of Margaret Podlich, Boat Owners Association, Subcommittee on Coast Guard and Maritime Transportation, House Committee on Transportation and Infrastructure, Hearing on Maritime Domain Awareness, December 9, 2009.

[30] DHS, *Small Vessel Security Strategy*, April 2008. For a critical review of this strategy, see DHS OIG, *DHS's Strategy and Plans to Counter Small Vessel Threats Needs Improvement*, September 2009.

[31] IOCs were authorized in the Security and Accountability for Every Port Act of 2006 (P.L. 109-347, sec. 108).

[32] 72 *Federal Register*, 3492 - 3604, January 25, 2007.

Author Contact Information

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

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

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