Transportation Security: Issues for the 111th Congress

David Randall Peterman
Analyst in Transportation Policy

Bart Elias
Specialist in Aviation Policy

John Frittelli
Specialist in Transportation Policy

January 28, 2009

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. In the 110th Congress, aviation, rail, and transit security were a major focus of congressional activity. At the end of July 2007, the House and Senate passed a conference agreement on H.R. 1 (H.Rept. 110-259) that was signed into law on August 3, 2007 as the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53). The act contains numerous provisions related to air, rail, and cargo security.

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 TSA and mandating a federalized workforce of security screeners to inspect airline passengers and their baggage. The act gave the TSA broad authority to assess vulnerabilities in aviation security and take steps to mitigate these risks. The TSA's progress on aviation security has been the subject of considerable congressional oversight. Aviation security policy and programs will likely be of considerable interest in the 111th Congress. Particular issues of interest include progress toward meeting the statutory mandate to screen all cargo placed on passenger airplanes by August 2010; deployment of next-generation checkpoint screening technologies; implementation of the Secure Flight system to check passenger data against the consolidated terrorist database; and options and proposals for strengthening security of large general aviation aircraft operations. While Congress passed legislation in the 110th Congress to extend the existing authorization of such sums as may be necessary for the 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 DHS reauthorization bill during the 111th Congress.

The vulnerability of passenger rail and transit systems to terrorist attacks is well documented. The 110th Congress significantly increased the federal role in securing those systems in the Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53), which authorized billions for rail and transit security grants, mandated security training for rail and transit workers, and authorized funding for more surface transportation security inspectors in the TSA.

A leading issue with regard to securing waterborne containerized cargo is the statutory mandate to scan all U.S. bound containers with non-intrusive inspection equipment at overseas ports of loading by July 2012. Debate over who should pay for cargo security, government or industry, and whether mandates or guidelines are the best approach to ensure industry's due diligence in protecting their supply chains are other leading issues. Hazardous materials (hazmat) transportation raises numerous security issues.

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 towards 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 principle 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 they did 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 they 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.

Aviation Security

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 TSA and mandating a federalized workforce of security screeners to inspect airline passengers and their baggage. The act gave the TSA broad authority to assess vulnerabilities in aviation security and take steps to mitigate these risks. The TSA's progress on aviation security has been the subject of considerable congressional oversight. Aviation security policy and programs will likely be of considerable interest in the 111th Congress. Particular issues of interest include progress toward meeting the statutory mandate to screen all cargo placed on passenger airplanes by August 2010; deployment of next-generation checkpoint screening technologies; implementation of the Secure Flight system to check passenger data against the consolidated terrorist database; and options and proposals for strengthening security of large general aviation aircraft operations. While Congress passed legislation in the 110th Congress to extend the existing authorization of such sums as may be necessary for the 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 DHS reauthorization bill during the 111th Congress.

A Risk-Based, Multi-Layered Approach

Aviation security policy since September 11, 2001, consists 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 the TSA has been criticized by some who believe that an overemphasis on allocating resources to screening airline passengers has left the system vulnerable to attacks 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 principle objectives of these measures are to prevent aircraft bombings and hijackings by terrorist passengers. However, the effectiveness of the TSA's implementation of virtually all of these security layers has been brought into question at some time or another since its creation.

Passenger Prescreening

Efforts to improve passenger prescreening have been impacted by concerns over the adequacy of measures to protect fliers' personal information and not infringe upon their civil rights. Critics have argued that the 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 the 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 the 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 have also delayed its deployment.

Provisions in the FY2008 Homeland Security Appropriations Act (P.L. 110-161), like prior appropriations measures, prohibit the TSA from fully deploying the *Secure Flight* program until these ongoing concerns are adequately addressed and also prohibit the use of commercial data or the transfer of passenger data to a non-federal entity. While commercial databases have potential to authenticate the identity of passengers, concerns have been raised about TSA's past handling of passenger data in a manner that was not fully explained to the public, leading to this restriction on

the transfer of personal data between the government and private entities other than the initial exchange of passenger name records from the airlines. A provision in P.L. 110-53 (section 1605) would require the TSA to submit to Congress a plan for testing and implementing an advanced passenger prescreening system to replace the current "no fly" and "selectee" lists distributed to airlines for vetting passengers.

The TSA has progressed with addressing the various concerns over traveler privacy, data retention, and reducing false positives, and on October 28, 2008, it published a final rule detailing the planned operational implementation of Secure Flight.[1] Under this regulation, the TSA will begin phasing in the use of Secure Flight to check passenger records against the consolidated terrorist database for domestic flights. In a second phase, the TSA will check passenger names for international departures and arrivals as well as overflights that cross through airspace overlying the 48 contiguous states, but do not land at a U.S. destination. Presently, passenger prescreening for international arrivals and departures is performed by U.S. Customs and Border Protection (CBP) using its Advanced Passenger Information System (APIS). However, overflights represent a new category of covered operations that will require transmission of passenger data for screening against the terrorist watch list and will encompass operators that may not operate flights to or from the United States. According to the final rule, the phase in of overflights in the Secure Flight system will coincide with the phase in of international flights, but a specific timeframe for this implementation has not yet been announced.

Provisions in P.L. 110-53 also required the DHS to establish appeals procedures for passengers misidentified though prescreening processes and establish an Office of Appeals and Redress that would be charged with implementing a "timely and fair process" for airline passengers delayed or denied boarding due to suspected misidentifications during the prescreening process. The 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 Internet online system, or by completing and mailing a complaint form. 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 111th Congress.

The TSA has also implemented a Registered Traveler (RT) program that is intended to expedite checkpoint screening of frequent fliers who voluntarily submit background information and biometric identifiers. While the TSA has approved RT programs operated by multiple vendors at several airports nationwide, it is up to individual airports to determine if they wish to participate in this program. As TSA moves forward with RT, the airline industry, which once backed this program as a means to reduce hassles for frequent fliers, now characterizes the manner in which has been implemented as having limited and questionable benefit. 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 has thus far only provided limited benefits and reductions in travel hassles to participants.

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

Passenger Screening

With regard to screening passengers, the TSA has struggled to strike a balance between effectively screening passengers for threat objects without causing undue delays and hassles to travelers. While the TSA is usually keeping passenger wait times below the stated objective of 10 minutes at smaller airports, average passenger wait times at major airports are typically greater. Further, audits of airport screening have concluded that screener performance still needs improvement. The Department of Homeland Security 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 screener performance. Also, the Government Accountability Office (GAO) has documented results of covert testing of airport security checkpoints demonstrating deficiencies in detecting improvised explosives and incendiary devices concealed on passengers and in their carry-on items, despite restrictions on carrying liquids and stepped-up measures for conducting secondary screening for explosives on passengers.[2]

The 9/11 Commission recommended that the TSA give priority attention to implementing technology and procedures for screening passengers for explosives, something not currently done routinely at screening checkpoints. Provisions to improve checkpoint technologies to detect explosives were included in the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458, hereafter the "Terrorism Prevention Act"). To address the issue of detecting explosives carried by passengers, the TSA pilot tested walk-through trace detection portals and has implemented procedures for conducting pat-down searches of passengers for explosives. Full deployment of the walk-through trace detection portals, or puffer machines, for use in secondary screening of selected passengers has been part of the TSA's strategy for screening passengers for explosives, but this initiative has been put on hold due to maintenance issues with deployed systems. The effectiveness of the strategy has also been brought into question by the recent foiled plot to bomb U.S.-bound airliners using liquid explosives. The TSA is working to identify strategies and technologies that more completely address the explosives threat posed by passengers and carry-on items. The TSA has since changed course with regard to its checkpoint technology investment and is now focusing heavily on field testing of: whole body imaging technologies using x-ray backscatter and millimeter wave imaging devices; advanced technology x-ray equipment capable of providing multiple view angles and automated threat detection capabilities to aid in the screening of carry-on items; and handheld bottled liquids scanners to screen for liquid explosives. During the 111th Congress, the TSA's investment and deployment strategies for these various next-generation checkpoint screening technologies is likely to be an issue of considerable interest.

Provisions in P.L. 110-53 (see section 1607) required the TSA to finalize its strategic plan for checkpoint explosives detection required by the Terrorism Prevention Act, and fully implement the plan within one year of enactment. The act also included provisions (see section 1612) that eliminated the cap on the system-wide number of TSA screeners, and called for specialized screener training on security skills, such as behavioral observation and analysis, explosives detection, and document examination. The act directs the TSA to hire sufficient personnel to

[2] 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.

ensure adequate aviation security and reduce average security-related delays to less than 10 minutes. The act also created a separate "Checkpoint Security Screening Fund," specifying that $250 million in security fees collected during FY2008 be deposited into this fund (see section 1601). While the fund was not reauthorized beyond FY2008, FY2009 appropriations for checkpoint technology, supplies, and other support was maintained at the $250 million level.

Federalization and Privatization of Airport Screening

A key issue in the debate over aviation security immediately following September 11, 2001, was whether airport security screeners should be federalized. At that time, airport screening operations suffered from high turnover, poor supervision and training, low wages, and a lack of regulatory oversight. All of these factors were believed to have contributed to a poor performing and highly vulnerable screening system. Federalizing the screener workforce was offered as a potential solution to address these deficiencies. However, while Congress ultimately resolved to federalize the screener workforce at most airports under ATSA, the act also set up a pilot program using contract screeners at five airports and gave all airports the option to request private screeners on an airport-by-airport basis starting November 19, 2004. There has been very little interest in this option among airports where federal screeners are deployed. One factor that may have limited airport interest in private screening is lingering 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 either request private screeners or continue using federal screeners and from any claims that may arise due to negligence or intentional wrongdoing on the part of airport security screeners, whether they be federal or private. Nonetheless, while the pilot program airports have all continued to use private screeners, interest in the TSA's Screening Partnership Program (SPP)—or opt-out program—for private screeners among other airports has been limited, and few have been fully converted to private screening operations.

Baggage Screening

While airports are, for the most part, meeting mandated requirements to inspect checked bags with explosive detection system (EDS) equipment 100% of the time, airports are continuing to struggle with the daunting task of integrating 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. Congress also gave the TSA the authority to issue letters of intent (LOIs) to airports, committing future funding toward in-line EDS integration projects. Despite these measures, efforts to integrate EDS systems at all airports is progressing slowly, prompting the 9/11 Commission to recommend that the TSA expedite installation of these in-line baggage screening systems.

Provisions to expedite and increase funding for in-line baggage screening were included in the Terrorism Prevention Act. However, meeting funding needs for airport security projects and setting priorities amid budgetary constraints remains an ongoing challenge for Congress. 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 in FY2008 through FY2011 for in-line baggage screening. The act also requires the TSA to prioritize airport projects based on risks and other considerations. Progress toward optimizing baggage screening systems at the nation's airports remains as a major aviation security issue for the 111th Congress.

Air Cargo Security

The Implementing the 9/11 Commission Recommendations Act of 2007 (P.L. 110-53, section 1602) requires 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 have been opposed by various stakeholders in the air cargo industry who believe that these requirements are overly burdensome and costly.[3] While the TSA has proposed a approach that relies heavily on shippers, cargo consolidators, and freight forwarders to carry out much of the operational aspects of screening cargo, sometimes at off-airport sites in conjunction with enhanced supply-chain security measures to prevent tampering with cargo after screening has been conducted, there has been some expressed over this approach. While the TSA maintains that this approach meets the requirements of the legislation, some have argued that the intent of the legislation was to have the TSA play a more direct role in overseeing screening operations, and that the screening would take place in closer physical proximity to locations where the cargo is loaded onto passenger airplanes.

The 9/11 Commission had also 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, 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 completed, the future direction for operational deployment of hardened cargo containers remains uncertain.

In addition to improving the screening of cargo placed on passenger aircraft, improvements in security programs for all-cargo operations have been required through regulations to protect against unauthorized access to large all-cargo aircraft. Under existing cargo security rules, secured areas of airports have been expanded to include cargo operations areas. These regulations also imposed 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. Also, under these regulations, an industry-wide database of known shippers has been established and is being maintained by TSA 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, concerns over the adequacy of security measures for these workers have been raised because, in some cases, airport workers are permitted to bypass airport 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

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

(P.L. 110-161), funding was provided to the TSA to carry out a pilot program to assess physical screening of airport employees. Based on the results of this testing, the 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 included statutory language establishing civil penalties when employers at airports fail to collect airport-issued security badges from employees whose airport jobs are terminated.

ATSA called for the TSA to explore the use of biometrics and other identification technologies for credentialing transport workers and the use of biometrics for airport access controls. While 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, the Terrorism Prevention Act required the TSA to issue guidance on the use of biometrics for airport access controls and the use of biometric technology to verify the identity of law enforcement officers authorized to carry firearms on passenger airliners. P.L. 110-53 included language requiring the TSA to report on its progress implementing access control measures for airline flight and cabin crew members and requires the 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). Progress toward achieving these objectives may be an issue of particular interest for the 111th Congress.

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 (FAMS) was greatly expanded under ATSA and air marshals are required on all high risk flights. In November 2003, FAMS was taken out of the TSA and realigned with the Bureau of Immigration and Customs Enforcement (ICE). However, the DHS Second Stage Review (2SR), issued in June 2005, proposed that the FAMS be placed back in the TSA, a proposal that Congress agreed to in report language accompanying the FY2006 DHS appropriations act. FAMS is once again part of the TSA. Recently, FAMS has been criticized by some current and former air marshals for procedures—such as dress codes and check-in procedures—that, they assert, compromise the covert mission of FAMS and place marshals and the traveling public at risk.

Despite the Bush Administration's initial reservations over allowing airline pilots to be armed, 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 Federal Flight Deck Officer (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 procedures to apply for the FFDO program are too cumbersome and the training site is too remote to accommodate many pilots interested in participating in the program. Some participants and observers have also voiced concerns that restrictive policies over carrying guns outside the cockpit potentially limit the program's effectiveness.

ATSA also mandated the implementation of hardened cockpit doors and stringent controls regarding access to the flight deck. The Terrorism Prevention Act contains a provision to study the use of secondary flight deck barriers—a concept United Airlines had been moving forward with 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 from possible bombings have also been raised in public policy debate regarding airline security. 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. The provision calls for pilot projects to test such technologies and also explore the use of deployable flight recorder devices and remote flight data-recording capabilities for security purposes. 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.[4]

The Shoulder-Fired Missile Threat

Concerns have also been raised over the potential threat to civil aircraft posed by shoulder-fired missiles (also known as Man-Portable Air Defense Systems, or MANPADS). Appropriations language in FY2003 directed the DHS to establish a program to evaluate the feasibility of adopting military aircraft anti-missile systems for use on passenger jets. This program is drawing to completion, and a final evaluation by the DHS addressing the technical feasibility, operational challenges, and cost-benefits of this approach is anticipated. Two contract teams, led by Northrop-Grumman and BAE Systems, developed prototype anti-missile systems for commercial airplanes for this program. Language in the Terrorism Prevention Act called for the FAA to implement an expedited process to certify the safety of these aircraft-based counter-MANPADS systems and also included language directing the administration to urgently pursue international arms-control agreements to limit the proliferation of MANPADS. In addition to the testing of aircraft-based counter-MANPADS systems, a smaller amount of funding was allocated for research on ground-based protection systems. In April 2006, the DHS issued a solicitation seeking alternative counter-MANPADS technologies for a demonstration project and recently awarded contracts for research and development efforts that will assess ground-based MANPADS countermeasures and other alternative mitigation options, in addition to the ongoing aircraft-based counter-MANPADS system development and evaluation initiative. While there is still some interest in funding alternative counter-MANPADS options, including ground-based systems, funding for research and development activities related to these technologies has so far been comparatively limited.

General Aviation Security

While some policymakers have expressed concern that security measures for general aviation aircraft are, in their estimation, very limited, general aviation operators have countered that they

[4] Federal Aviation Administration, "Security Related Considerations in the Design and Operation of Transport Category Airplanes; Proposed Rule," *Federal Register, 72*(3), pp. 629-639, January 5, 2007.

have been overburdened by unnecessary airspace and airport restrictions. General aviation restrictions are most prevalent in the Washington, DC area, where the city is encircled by a 15-mile radius flight restricted zone (FRZ) in which general aviation operations are significantly limited, and a larger air defense identification zone (ADIZ) where 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—to resume at Washington Reagan National Airport (DCA) which is located at the center of the flight restricted area. Operations at smaller GA airports located within the 15-mile FRZ are highly restricted, requiring pilots to undergo thorough 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 Disney 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. General aviation advocates also point to a large number of restricted airspace violations—more than 1,000 per year since the terrorist attacks of 2001—as evidence that security-related restrictions are overly complex and too broad in scope. Almost one-half of these violations occurred in the airspace around Washington, DC, where complex communications procedures have been put in place over a wide area. The FAA reduced the size of the Washington ADIZ 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 this new speed restriction, which exceeds the capability of most small, light piston-powered aircraft, and is largely designed to aid in early detection of fast-moving aircraft that may pose a threat to critical sites in the Washington, DC, area.

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 the pilot community to detect and report suspicious activity. In the area of flight training, flight training providers are engaged in verifying citizenship or confirming that background checks have been properly completed by the TSA before providing training to foreign nationals, as mandated under P.L. 108-176. A provision in the Terrorism Prevention Act would allow aircraft leasing and charter companies to voluntarily provide the 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 the TSA to develop and implement a standardized risk assessment program at GA airports. Provisions in the bill also call for establishing a grant program to enhance security at GA airports, if such a program is deemed feasible, and requires inbound international flights using GA aircraft to submit passenger information and advance flight notification to CBP prior to entering U.S. airspace for vetting against appropriate databases.

In October 2008, The TSA proposed that general aviation reliever airports, that relieve congestion from major commercial airports, and general aviation airports that regularly serve scheduled commuter flights and public charter operations must adopt a security program. 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 public regarding airport security matters through public advisories, and establish a system for maintaining security-related records of law enforcement response to incidents that occur at the airport. The TSA has also proposed to implement a variety of security measures for operators of all large general aviation aircraft, weighing more than 12,500 pounds, including privately-owned, fractionally-owned, and corporate aircraft. These measures would include: fingerprint-based criminal history records checks (CHRCs) 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 kg (roughly 100,000 pounds) would be required to screen passengers and their accessible property. [5] Similar security measures are already required for charter operators. However, large aircraft operators and airports have expressed concern over the burden that would be imposed by these proposals addressing general aviation operations that have not previously been the subject of security-related regulations. **(CRS contact: Bart Elias)**

Transit and Passenger Rail Security

Bombings of passenger train 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 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, there are steps that can be taken to reduce the risks, as well as the consequences, of an attack. These include conducting vulnerability assessments; emergency planning; and emergency response training and drilling of transit personnel, ideally in coordination with police, fire, and emergency medical personnel. Additional options include increasing the number of transit security personnel, installing video surveillance equipment in vehicles and stations, and conducting random inspections of passengers' bags, platforms, and trains visually and with the aid of bomb-sniffing dogs.

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

[5] 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.

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.

DHS announced that 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, were completed on May 21, 2007. 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."[6]

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, and $275 million for FY2007; for FY2008, Congress provided $400 million, plus $11.5 million for Over-the-Road Bus security grants and $16 million for trucking industry security grants.

The Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53), passed by Congress on July 27, 2007, includes provisions on passenger rail and transit security. These include authorizing $3.5 billion over the period FY2008-FY2011 for grants for public transportation security, of which $840 million can be used 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, DC (section 1515), and $132 million is 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 would be required to have security plans approved by DHS (sections 1405 and 1512).

Other provisions include funding for TSA to hire up to 100 more surface transportation security inspectors (section 1304); currently TSA has 100 such inspectors, requiring 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 giving DHS the authority to regulate rail and transit employee security training standards (sections 1408 and 1517). **(CRS contact: David Randall Peterman)**

Truck, Rail, and Marine Cargo Security

Imported Cargo

Of particular concern is ensuring the integrity of imported cargo. More than 11 million marine containers from all corners of the globe arrive at U.S. seaports annually, while 11 million truckloads and more than 2 million railcars arrive at U.S. land border crossings. Since the September 11, 2001 attack, Customs and Border Protection (CBP) has issued new requirements requiring freight carriers to report cargo manifests (shipment information) before they reach U.S. borders. Container ships must report shipment details on each container 24 hours before it is

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

loaded at a foreign port. Truckers from Canada and Mexico must report their trailers' contents from 30 minutes to an hour prior to border arrival and railroads must report this information two hours prior to border arrival. CBP analyzes the cargo manifests and other intelligence to select which cargo units to physically inspect. CBP's selection process is thus critical in keeping terrorists and their weapons from being smuggled into the country.

100% Scanning Requirement

In its oversight role, Congress is scrutinizing CBP's cargo inspection process. In the Port Security Improvement Act (P.L. 109-347), Congress required DHS to evaluate whether additional cargo information is needed to evaluate shipment risk and required DHS to reexamine its targeting system to determine where improvements to the system could be made. On November 25, 2008, CBP published a final rule requiring importers to submit an additional ten items that will provide more information on the overseas origin and the buyers and sellers involved in a container shipment.[7] Congress also required DHS to set up a pilot program at three overseas ports to test the feasibility of scanning all U.S.-bound containers at those ports, a program DHS refers to as "The Secure Freight Initiative." The Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53, section 1701), requires that all imported containers be scanned by nonintrusive imaging equipment and radiation detection equipment at a foreign loading port by July 1, 2012, but the Secretary of DHS may extend the deadline at a port or ports by two-year increments if two of the following six conditions are met:

- scanning systems are not available for purchase and installation;
- scanning systems do not have a sufficiently low false alarm rate for use in the supply chain;
- a port does not have the physical characteristics to install a scanning system;
- scanning systems cannot be integrated with existing systems;
- scanning systems will significantly affect trade capacity and the flow of cargo; and
- scanning systems do not adequately provide an automated notification of questionable or high-risk cargo as a trigger for further inspection by trained personnel.

Proponents of 100% scanning argue that the manifest information CBP relies on to flag which containers to scan is simply not an adequate basis for determining risk and thus requiring all containers to be scanned is necessary. Container shippers and carriers have argued that 100% scanning will severely bottleneck port operations, not only because of the time required to scan a container but more significantly, the time required for a customs official to analyze the results of a container scan. Opponents of 100% scanning also assert that current scanning equipment is not accurate enough and could be relatively easily circumvented by terrorists.

[7] See 73 FR 71729.

Private Industry's Role

Because most surface and marine freight transportation assets are owned by private industry, and because there are too many shipments for government to monitor on its own, government officials have to rely extensively on private industry to tighten control over their supply chains. Industry has taken steps to protect their operations from terrorist infiltration. The Association of American Railroads has conducted a security risk assessment that prioritizes the industry's assets and lists countermeasures to be taken at different alert levels. Railroads have also created a "Railway Alert Network" that is designed to make sure individual railroads receive timely threat information. Barge operators have created a "Model Vessel Security Plan" through their industry association, the American Waterways Operators. The American Trucking Associations has expanded a "Highway Watch" program to include training for drivers on how to spot suspicious activity. Intermodal (container) shippers have created a "Smart and Secure Trade Lanes" program to evaluate anti-tampering and tracking devices for marine containers. An issue for policymakers is determining the best approach for ensuring private industry's cooperation and due diligence over the long term. For example, policymakers are evaluating which security measures should be mandated versus which ones should be issued as guidelines or "best practices." How to validate that the agreed upon security measures are in fact being carried out by industry is also an issue. CBP's Customs Trade Partnership Against Terrorism Program (C-TPAT) provides incentive for importers and carriers to take specified actions to safeguard commerce by offering expedited customs clearance for industry participants. In its oversight role. Congress will likely continue to assess the effectiveness of this program.

Paying for Cargo Security

Freight carriers and shippers are private, for-profit corporations, which raises the issue of whether they or general taxpayers should pay for security improvements. Advocates for public funding argue that homeland security is a national concern and therefore a federal government responsibility that should be paid for from the General Treasury. Others argue that carriers and shippers are the direct beneficiaries of improved cargo security. They argue that it is in their own economic interest to protect their assets from terrorist attack, that additional security measures also deter cargo theft which is costly to the freight industry, and that therefore they should bear the cost of security improvements. Several legislative efforts to establish a security fee paid by industry to generate funds for a federal port security grant program have failed in Congress. Meanwhile, some ports and freight carriers are beginning to add security surcharges to their freight invoices while other carriers are presumably incorporating extra security-related costs in their freight rates.

Transportation Worker Identification Credential Program

On January 25, 2007, the TSA and Coast Guard issued a final rule for implementing the Transportation Worker Identification Credential (TWIC) at U.S. ports.[8] Longshoremen, port truck drivers, merchant mariners, and other maritime workers 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 on each worker before issuing a

[8] *Federal Register*, v. 72, no. 16, January 25, 2007, pp. 3492 - 3604.

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 that is intended 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 conducting a pilot test at a handful of ports to determine the best kind of card reader technology to require. The Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53, section 1309) codifies in statute a list of criminal offenses that would disqualify a worker from obtaining a TWIC card, but allows the Secretary of DHS, by rulemaking, to add to or modify the list of disqualifying offenses. These offenses were included in the final regulation issued by DHS on January 25, 2007.

Cargo Visibility

A leading issue with regard to securing truck, rail, and waterborne cargo is to what extent government authorities need the capability to track a given shipment at a particular time. Much of the attention with regard to cargo visibility concerns the tracking of marine shipping containers. Marine containers are not currently outfitted with tracking devices, but it is common practice to seal container doors with tamper-evident fixtures. Security officials are concerned that a particularly vulnerable stage in the container shipping process occurs when containers are trucked to the overseas port of loading or when they are trucked from the U.S. port of unloading to their final U.S. destination. At this stage, the integrity of the shipment rests solely with the trustworthiness or due diligence of the truck driver. A sensor or tracking device could help ensure the integrity of container shipments during these vulnerable stages. Since the September 11, 2001 attack, there has been rapid development of palm-sized tracking devices and sensors that could be inserted on an interior wall of a container. However, while this so-called "smart-box" technology is being tested in selected routes, it has not been resolved whether and how best to deploy it on a widespread basis. In the near term, shippers and carriers favor using the best container seals currently in use rather than moving to the more costly sensor and tracking devices. Congress is likely to continue its oversight of the technological development of container security devices and debate whether these devices can be effectively deployed to improve cargo security. **(CRS contact: John Frittelli)**

Hazmat Cargo Security

Hundreds of thousands of trucks and railroad tank cars transport tons of hazardous materials (hazmat) daily. These shipments can be used as instruments or targets of terror. There is a virtually unlimited number of ways that the hazmat transportation system is at risk from terrorists. For example, tank trucks can be attacked, drivers can be killed, and loads can be hijacked and released during shipment. Simply put, there are too many points of vulnerability to *ensure* security during hazmat transportation. A major challenge is to cost effectively increase the security of these shipments, especially those that pose the most danger to the public, while still meeting, to the extent possible, the transportation requirements of commerce.

Industry and government are gradually implementing a "layered" system of measures affecting shippers, carriers, and drivers to reduce associated security risks. This system involves incident prevention, preparedness, and response. The Departments of Transportation (DOT) and Homeland Security (DHS) have taken actions to enhance the security of hazmat transportation.

For example, DOT requires shippers and carriers to implement security plans regarding specified hazmat transportation. DOT grants encourage state and some local governmental personnel to conduct hazmat inspections and to plan and train for spills of these materials. Also, this Department has contacted thousands of companies that are seeking to improve their security programs, and has established communication links with industry.

DHS conveys threat information to law enforcement and industry, and conducts vulnerability assessments. DHS administers a grant that provides for the training and communications infrastructure which truck drivers, highway workers, and others use to report potential security threats and safety concerns on the Nation's roads. DHS screens commercial drivers applying for an endorsement to carry hazardous materials to determine whether a driver poses a security threat necessitating denial of the hazmat endorsement. DHS has also deployed radiation detection equipment at interstate truck inspection stations. Whether the pace of these actions is adequate or not is subject to debate. It is widely recognized that more could be done to promote hazmat transportation security, but additional costs would be incurred and tradeoffs would need to be considered.

There remain many issues associated with hazmat transportation security. Many Members of Congress want to know whether current federal policies, regulations, and grants could more effectively promote hazmat transportation security at reasonable costs. There are issues regarding routing of hazmat through urban centers and debate persists over the pros and cons of rerouting high hazard shipments. Requiring tracking devices for hazmat shipments and limiting security requirements to just those hazardous commodities that are potentially the most dangerous are also topics of debate. Other options include increased security awareness training for state truck inspectors and certain employees of truck leasing companies, and requiring enhanced security plans and communication systems for carriers of high hazard materials shipments beyond those now required. Each of these options poses costs that need to be evaluated within the context of other investments.

The Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53) requires DHS, in consultation with the DOT, to develop a program to encourage railroads to equip their railcars carrying "security-sensitive" materials with tracking devices indicating their location and condition (see section 1552). The act requires railroads to annually compile data on certain hazardous materials shipments, provide a written analysis of the safety and security risks associated with those shipments, and identify any practical alternative routes that may be more safe and secure, including routes that involve interchange agreements with other railroads (see section 1551). Regarding the trucking of hazardous materials (hazmat), the act requires DOT, in consultation with DHS, to review existing hazmat routes and develop criteria based on safety and security concerns to assist states in designating routes for hazmat transportation (see section 1553(a)). The act requires DOT to assess whether route plans currently required for trucks carrying radioactive or explosive materials should also be required for trucks carrying other types of hazmat (see section 1553(b)). The act requires DHS, in consultation with DOT, to develop a program to facilitate the tracking of "security-sensitive" material shipments (see section 1554). **(CRS contact: John Frittelli)**

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