Congressional Research Service

Report RL33512

Transportation Security: Issues for the 110th Congress

David Randall Peterman, Bart Elias, and John Frittelli, Resources, Science, and Industry Division

January 22, 2008

Abstract. 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 have been 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.

Transportation Security: Issues for the 110th Congress

David Randall Peterman
Analyst in Transportation Policy

Bart Elias
Specialist in Aviation Policy

John Frittelli
Specialist in Transportation Policy

January 22, 2008

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 have been 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 Transportation Security Administration (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. P.L. 110-53 extends the existing authorization of such sums as may be necessary for the TSA's aviation security functions through FY2011.

The vulnerability of passenger rail systems to terrorist attacks is well documented. Steps that can be taken to reduce the risks and consequences of an attack include vulnerability assessments, emergency planning, and emergency response training and drilling of transit personnel, ideally in coordination with police, fire, and emergency medical personnel. A leading issue with regard to securing truck, rail, and waterborne cargo is the desire of government authorities to track a given freight shipment at any time, particularly the tracking of marine containers as they are trucked to and from seaports. Security experts believe this is a particularly vulnerable point in the container supply chain. 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 110th Congress as funding authorization for most of the TSA's aviation security functions expired at the end of FY2006, and others are set to expire at the end of FY2007. Both the House and the Senate have passed legislation 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).

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 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.

Recently, privacy advocates have raised considerable concerns over the Automated Targeting System (ATS), a data-mining program for assessing the risk of all international travelers, as well as freight carried on international flights. Recent public disclosure regarding the scope of this program and associated data collection and data retention policies, in November 2006, have renewed debate over whether certain passenger information collection and analysis practices unduly infringe upon privacy rights, or whether they are necessary actions to assess terrorism risks to aviation. Provisions in P.L. 110-53 would require the DHS to 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 TSA has also implemented a Registered Traveler (RT) program that is intended to speed the passage through security checkpoints of frequent fliers who voluntarily submit background information and biometric identifiers. Initial trials of the RT program concept concluded in October 2005, and the TSA has launched RT programs operated by multiple vendors at several airports nationwide. According to the TSA, 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 it is being implemented as having limited and questionable benefit. Lingering concerns are that the program is not universal, nor is it available at all airports. Also, use of the program as a testbed for streamlined screening technologies and procedures has thus only provided limited benefits and reductions in travel hassles to participants. While the potential benefits of the RT program have not been fully realized, Congress has included language in the FY2008 Consolidated Appropriations Act (P.L. 110-161) directing the TSA to establish an international RT program that incorporates biometrics and e-passport technologies to be used in conjunction with US VISIT and the Visa Waiver Program. Under the existing RT program, some international carriers have been participating for outbound flights originating from JFK and Newark Liberty airports.

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) 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.[1]

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.

Provisions in P.L. 110-53 (see section 1607) would require the TSA to finalize within 30 days the 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 contains provisions (see section 1612) that would eliminate the cap on the system-wide number of TSA screeners, and would require specialized training for screeners on security skills such as behavioral observation and analysis, explosives detection, and document examination. The act directs the TSA to hire sufficient personnel to ensure adequate aviation security and reduce average security-related delays to less than 10 minutes. The act creates a separate "Checkpoint Security Screening Fund," specifying that $250 million in security fees collected during FY2008 be deposited into this fund (see section 1601). Amounts deposited into the fund would be available for research, development, deployment, and installation of equipment to improve the detection of explosives at passenger checkpoints. The act also directs the TSA to carry out a pilot study to examine technologies to improve the security at exits to airport secured areas (see section 1613).

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

[1] 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.

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 only one has been fully converted to private screening operations since the program was made available.

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, in contrast to authorization language in Vision 100 (P.L. 108-176) that set federal funding levels for aviation security capital projects at 90% for large and medium hubs and at 95% for all other airports, appropriations language (see P.L. 109-90; P.L. 109-295) has limited the federal share of project costs under LOIs to 75% for medium and large hubs, and 90% for all other airports in FY2006 and FY2007. 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 would extend authority for mandatory funding of the Aviation Security Capital Fund through 2028, would authorize an increased discretionary funding level of $450 million in FY2008 through FY2011 for in-line baggage screening, and would require the TSA to prioritize airport projects based on risks and other considerations (see sections 1603 and 1604).

Air Cargo Security

Some Members of Congress have voiced concerns that, while 100% of passenger baggage is required to be screened, only a relatively small amount of cargo carried on passenger airplanes is physically inspected. The 9/11 Commission recommended that TSA intensify its efforts to identify, track, and screen potentially dangerous cargo. Congress responded by increasing funding for air cargo security operations and research to $115 million in FY2005, compared to $85 million in FY2004, and designating funds for expanding the known shipper program for vetting shipments on passenger aircraft; increasing oversight of cargo security; and continuing research and development of technologies to improve air cargo security. In both FY2006 and FY2007, funding for air cargo security operations was set at $55 million. For FY2008, the amount was increased to $73 million to increase the training and deployment of canine teams for cargo screening and deploy additional cargo security inspectors. Language in the FY2008 DHS appropriations act also directs the TSA to work with other DHS components to develop technologies that will aid in achieving 100% screening of all cargo placed on passenger airliners

and to work with industry to increase the use of EDS equipment for cargo screening. The Implementing the 9/11 Commission Recommendations Act of 2007 (P.L. 110-53, section 1602) contains a provision that would require screening of all air cargo placed on passenger aircraft, 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. The provision would phase-in the percentage of cargo required to be inspected, setting these levels at 50% within 18 months, and 100% within three years of enactment. The measure is opposed by various stakeholders in the air cargo industry that believe its requirements are overly burdensome and costly.[2]

The 9/11 Commission also recommended deploying at least one hardened cargo container on each passenger airliner for carrying suspect cargo. While this recommendation was reflected in a Terrorism Prevention Act provision mandating a study of the proposal to deploy blast-resistant cargo containers, the 9/11 Commission noted that this is progressing slowly. P.L. 110-53 contains a provision that would require the DHS to complete its evaluation of this pilot program by January 1, 2008, and, based on this evaluation, provide hardened cargo containers for risk-based deployment 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 hardened containers are designed to mitigate the threat of a terrorist bomb carried in a cargo shipment or luggage, some policymakers believe that the only effective way to mitigate such a threat is to screen all cargo placed on passenger aircraft as is currently done for checked baggage. As noted above, P.L. 110-53 contains a provision that would require 100% physical inspection of all cargo placed on passenger aircraft within three years. The TSA, however, has cautioned that such an approach is not technically and logistically feasible at the present time without unduly impacting cargo operations on passenger aircraft. The TSA has instead proposed a strategic plan calling for the use of risk-based prescreening techniques to identify cargo for targeted inspection or exclusion from carriage on passenger aircraft and a threefold increase in random inspections. The TSA has been working on a freight assessment system for assigning risk to cargo shipments and targeting screening and inspection efforts on elevated risk cargo. It is anticipated that the TSA will introduce this system sometime in FY2008.

In addition to improving the screening of cargo placed on passenger aircraft, improvements in security programs for all-cargo operations are planned to protect against unauthorized access to large all-cargo aircraft. Under new cargo security rules, secured areas of airports are being expanded to include cargo operations areas thus requiring criminal background checks and security threat assessments for an estimated 50,000 additional airport workers. The new regulations also impose requirements on freight forwarders that ship by air (referred to as indirect air carriers) and require security threat assessments for 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.

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

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. Report language accompanying both the Senate (S. 1644; S.Rept. 110-84) and the House (H.R. 2638; H.Rept. 110-181) The FY2008 Consolidated Appropriations Act (P.L. 110-161) provides funding to the TSA to carry out a pilot program to assess physical screening of airport employees. The act also includes statutory language establishing civil penalties when employers at airports fail to collect airport-issued security badges from employees whose airport jobs are terminated.

ATSA also 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 includes language that would require the TSA to report on its progress implementing access control measures for airline flight and cabin crew members and would 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). Another provision in P.L. 110-53 (section 1616) would suspend further certification of foreign repair stations one year after enactment, unless and until required security regulations are put in place and regulatory compliance audits of repair station facilities are carried out by TSA inspectors.

In-Flight Security Measures

Existing in-flight security measures consist primarily of federal air marshals, armed pilots on some flights, 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, the Federal Air Marshal program 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 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. H.R. 3925 seeks 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) includes 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.[3]

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 evaluating the feasibility of adopting military aircraft anti-missile systems for use on passenger jets. This program is still ongoing. Two contract teams, led by Northrop-Grumman and BAE Systems, are developing prototype anti-missile systems. Language in the Terrorism Prevention Act calls for the FAA to implement an expedited process to certify the safety of aircraft-based counter-MANPADS systems and also includes language directing the administration to urgently pursue international arms-control agreements to limit the proliferation of MANPADS. FY2007 DHS appropriations (P.L. 109-295) provided $40 million for counter-MANPADS research and development. Of this, $35 million is designated for evaluating the suitability of aircraft-based systems in the airline industry. This appropriation is down from the FY2006 level of $110 million, reflecting a shift from a technology development effort to a technology evaluation phase during FY2007. In addition to the funding of aircraft-based counter-MANPADS systems, a smaller amount of funding has been allocated for research on ground-based protection systems. In April 2006, the DHS issued a solicitation seeking alternative counter-MANPADS technologies for a

[3] 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.

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 initiatives. It is expected that operational testing of aircraft based counter-MANPADS systems will conclude in FY2008, and the TSA will provide an evaluation of the performance of these systems. 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, weak and practically non-existent, general aviation operators have countered that they 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.

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.

Also, about one-quarter of airspace violations have occurred in airspace temporarily restricted 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. 109-176. 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) requires 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 and implement it on a risk-managed basis 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. **(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 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."[4]

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

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), of which $200 million is 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

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.

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 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.

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.[5] 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.

[5] DHS has proposed that an additional 12 data items be submitted by maritime importers and vessel carriers, see 73 FR 90.

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. With regard to CBP's Customs Trade Partnership Against Terrorism Program, Congress requested DHS to conduct a pilot program to test whether third party entities could be used to validate shippers' compliance with the program.[6]

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. The Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53, section 1308) requires DHS to conduct a study of the need for and feasibility of creating a user fee in the maritime and surface modes for funding transportation security improvements.

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.[7] Longshoremen, port truck

[6] See section 218 of P.L. 109-347.

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

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 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 $137 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 considering whether to incorporate the TWIC system into all modes of transportation. As TWIC is being implemented, issues for Congress include what affect it could have on the near-term supply of port workers.

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. **(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