Order Code IB10135

Transportation Security: Issues for the 109th Congress

Updated December 7, 2005

John Frittelli, Coordinator
Resources, Science, and Industry Division

CONTENTS

SUMMARY

MOST RECENT DEVELOPMENTS

BACKGROUND AND ANALYSIS
- Aviation Security
  - A Risk-Based, Multi-Layered Approach
  - Passenger Prescreening
  - Passenger Screening
  - Federalization and Privatization of Airport Screening
  - Baggage Screening
  - Air Cargo Security
  - Airport and Aircraft Access Controls
  - In-Flight Security Measures
  - The Shoulder-Fired Missile Threat
  - General Aviation Security
  - Related Legislation in the 109th Congress
- Transit and Passenger Rail Security
- Truck, Rail, and Marine Cargo Security
  - Cargo Visibility
  - Imported Cargo
  - Private Industry's Role
  - Paying for Cargo Security
  - Selected Legislation in the 109th Congress
- Hazmat Cargo Security

CONGRESSIONAL HEARINGS, REPORTS, AND DOCUMENTS
- Non-Mode Specific
- Aviation
- Transit
- Surface and Marine Cargo

FOR ADDITIONAL READING

Transportation Security: Issues for the 109th 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, reasonable measures can be taken to deter terrorists. The focus of this issue brief is how best to construct and finance a system of deterrence, protection, and response that effectively reduces the possibility and consequences of another terrorist attack without unduly interfering with travel, commerce, and civil liberties.

Aviation security has been a major focus of transportation security policy following the terrorist attacks of September 11, 2001. In the aftermath of these attacks, the 107th Congress moved quickly to pass the Aviation and Transportation Security Act (ATSA; P.L. 107-71) creating the Transportation Security Administration (TSA) and mandating a federalized workforce of security screeners to inspect airline passengers and their baggage. The 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 over the past four years. Aviation security policy and programs continue to be of considerable interest in the 109th Congress.

The July 2005 bombing of trains in London and the bombings of commuter trains and subway trains in Madrid and Moscow in 2004 highlighted the vulnerability of passenger rail systems to terrorist attacks. The volume of ridership and number of access points make it impractical to subject all rail passengers to the type of screening airline passengers undergo. Nevertheless, there are prudent steps that can be taken to reduce the risks, and consequences, of an attack. These include vulnerability assessments; emergency planning; and emergency response training and drilling of transit personnel, ideally in coordination with police, fire, and emergency medical personnel, as well as purchase of communication and safety equipment. Additional options include increasing the number of transit security personnel, installing video surveillance equipment in vehicles and stations, and conducting random inspections of platforms and trains using bomb-sniffing dogs.

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 a particular time. Most of the attention with regard to cargo vulnerability concerns 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. 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.

MOST RECENT DEVELOPMENTS

Two transportation security bills have been reported out of committee. The Senate Committee on Commerce, Science, and Transportation reported the Transportation Security Improvement Act of 2005 (S. 1052) on November 17, 2005. The bill focuses on land and maritime modes and, among other provisions, would provide grants for bus, freight and passenger rail security upgrades; encourage the development of tracking devices for hazardous materials shipments; require the development of security-training guidelines for employees of short-term truck leasing companies; and advance the timing that maritime importers provide shipment entry data to customs. On the same day, the Senate Committee on Banking, Housing, and Urban Affairs reported the Public Transportation Terrorism Prevention Act of 2005 (S. 2032) which would authorize federal grants to transit agencies for both capital and operational security improvements that would be allocated based on priorities identified in risk assessments.

The Administration has issued national strategies regarding transportation security. In September 2005, the Department of Homeland Security (DHS) delivered a classified report to Congress on a "National Strategy for Transportation Security." Also in September 2005, DHS announced the completion of a national strategy for maritime cargo security and in October 2005 announced the completion of eight action plans to implement the maritime security strategy. During committee hearings held in July 2005 on the reorganization of DHS, Secretary Chertoff discussed a "Secure Freight" initiative that would incorporate additional shipment documentation to better target higher risk or unknown risk marine containers for inspection.

The 9/11 Commission issued its final report on December 5, 2005 and graded the federal government's progress in implementing its various recommendations. The Commission issued Congress a failing grade for not allocating homeland security funds based on risk, a grade of "B" for not fully giving the House and Senate homeland security committees exclusive jurisdiction over all counterterrorism functions of the DHS, a "C minus" regarding DHS's "National Strategy for Transportation Security," an "F" for airline passenger pre-screening, a "C" for airline screening explosive detection, and a "D" for airline checked baggage and cargo screening.

BACKGROUND AND ANALYSIS

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. The difficulty and cost of protecting the transportation sector from terrorist attack raises a core question confronting 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, reasonable measures can be taken to deter terrorists. The focus of this issue brief 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. Terrorists 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.

A narrower set of policy questions is how to tailor an anti-terrorism strategy that corresponds with the service requirements of each particular mode. For instance, while prescreening all airline or cruise ship passengers is possible, pre-screening all transit riders is practically impossible. Likewise, inspecting 100% of imported marine cargo is practically impossible, so inspectors rely heavily on shipment documentation to select which shipments to examine more closely. The issue for policymakers is deciding whether ensuring the trustworthiness of the passengers and cargo flowing through each mode of transportation can be reasonably achieved and, if so, how best to achieve it without impeding travel and commerce. Another issue is ensuring the trustworthiness of the companies that operate in the system. The TSA's "known shipper" program for cargo carried aboard passenger planes and Customs and Border Protection's (CBP) "Trade Partnership Against Terrorism" (C-TPAT) program for cargo imported by all modes are initiatives designed to ensure the trustworthiness of the companies that operate in the system. These two programs essentially require the companies that routinely operate in their respective transportation systems to vouch for the trustworthiness of each other and to alert authorities when they spot any anomalies or suspicious activity. A point of contention is to what extent government can rely on the transportation industry to exercise due diligence in protecting their operations from terrorist attack. In addition to the integrity of transportation companies, there is also the issue of the trustworthiness of their employees. As requested by Congress, the TSA is developing a universal biometric transportation worker ID card that is intended to restrict access to sensitive areas within transportation facilities. One unresolved issue is deciding what should disqualify a transportation worker from obtaining a card. What sort of background would make someone a "security risk?"

The 109th Congress is debating other areas of disagreement with regard to transportation security. It is debating whether the nation is doing enough, and is acting in a timely fashion, to secure transportation systems, particularly for non-aviation modes of transportation. It is debating financial issues, such as what level of spending will buy what level of security and who should pay for security: federal taxpayers, state and local governments, system users, or some sort of cost share arrangement among all of the above. How federal security dollars should be allocated across the country is a focal point of the debate. In its oversight role, Congress continues to examine the effectiveness of DHS initiatives to strengthen

transportation security, including the degree of coordination among agencies within DHS towards that effort.

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 over the past four years. Aviation security policy and programs continue to be of considerable interest in the 109th 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 on board, 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 by some or at some time over the past four years.

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 remain over data protections and redress procedures for passengers falsely identified by the system and have delayed its deployment as well. Provisions in the FY2006 Homeland Security Appropriations Act (P.L. 109-90) 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. The TSA is also evaluating trials of a Registered Traveler (RT) program designed to speed the passage through security checkpoints of frequent fliers who voluntarily submit background information and biometric identifiers. The RT trials concluded in October 2005, but the TSA has indicated that a nationwide RT program should be up and running by early summer 2006. According to the TSA, it will be up to individual airports to determine if they wish to participate in the future RT program. Trials of a public-private partnership similar to the RT program are still ongoing at Orlando International Airport and this pilot is expected to continue through mid-2006.

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 in most airport checkpoint queues, 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. Furthermore, 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. To address this recommendation, the TSA is pilot testing walk-through trace detection portals and has implemented procedures for conducting pat-down searches of passengers for explosives. 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").

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. While several airports have expressed an interest in private screening, they are being cautious in proceeding because the TSA has offered few details and limited guidance on how private screening will be implemented. Another factor that has limited airport interest in private screening has been lingering liability concerns. 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.

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 authorizing up to $500 million per year through FY2007 and provided the TSA with 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. In contrast to authorization language in Vision 100 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) limits the federal share of project costs under LOIs to 75% for medium and large hubs, and 90 percent for all other airports. Meeting funding needs for airport security projects and setting priorities amid budgetary constraints remains an ongoing challenge for Congress.

Air Cargo Security. Some Members of Congress have voiced concerns that, while 100% of baggage is required to be screened, only a relatively small amount of cargo carried on passenger airplanes is screened or 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 designated 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 FY2006 funding for air cargo security dropped back down to $55 million for operations plus an additional $30 million set aside for three cargo screening pilot programs that will be carried out by the S&T directorate under the new consolidation of DHS research and development activities. Language in th FY2006 DHS appropriations act also directs the TSA to work with other DHS components to develop technologies that will aid in meeting the objective of screening 100% of all cargo placed on passenger airliners. Despite the drop in funding levels compared to FY2005, this funding provides for an additional 100 air cargo security compliance inspectors.

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, this study has not yet been funded or commenced. 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. 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. 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. While the TSA has issued a proposed regulatory framework for the implementation and oversight of security at air cargo and air freight forwarding facilities, these regulations have not been finalized despite a statutory requirement in the Terrorism Prevention Act to do so by September 2005.

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 has been questioned because, in some cases, airport workers have been 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. 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. 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.

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.

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 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 appropriated $27 million for FY2006 to administer the program and conduct initial training for about 100 pilots every week. However, there are lingering concerns that the procedures to apply for the program are too cumbersome and the training site is too remote to accommodate many pilots interested in participating in the program and that restrictive policies over carrying guns outside the cockpit potentially limit the program's effectiveness.

ATSA 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 is moving

forward with on its own initiative — to overcome 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.

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, and a evaluation of the prototype systems is expected to be completed by January 2006. FY2006 DHS appropriations (P.L. 109-90) provides $110 million for the continued evaluation and refinement of these aircraft-based countermeasures, but did not set aside any of this funding for exploring alternative technologies as proposed by the House. Language in the Terrorism Prevention Act calls for the FAA to implement an expedited process to certify the safety of such 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.

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 in which general aviation operations are significantly limited, and a larger air defense identification zone 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 and other 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. 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 before providing training to foreign nationals. 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.

Related Legislation in the 109th Congress. Several aviation security-related measures have been introduced in the 109th Congress. The Department of Homeland Security Authorization Act for FY2006 (H.R. 1817) contains two provisions related to

aviation security: a provision prohibiting any increases in aviation security-related fees and a provision that would require the TSA to implement a security plan to resume general aviation flights at Washington Reagan National Airport (DCA). The TSA has implemented a plan allowing general aviation and charter flights to resume at DCA under strict security measures including picking up air marshals and inspecting the aircraft at designated "gateway" airports. Representative Markey has offered the Strengthen Aviation Security Act (H.R. 2649) which endeavors to improve aviation security by: phasing-in 100% screening of cargo carried on passenger airplanes; establishing no-fly zones around sensitive nuclear and chemical facilities during periods of heightened terror alert; and requiring vulnerability assessments and security enhancements at general aviation airports. The bill also would: require installing cockpit doors and partitions on all-cargo aircraft; provide for training of law enforcement officers who travel armed on commercial flights; require enhanced background checks and physical screening of airport workers; and establish whistleblower protections for aviation security workers. Representative Markey also introduced the Air Cargo Security Act (H.R. 2044) which would require regular inspections of shipping facilities and security training for cargo handlers. Additionally, Representative Oberstar introduced the Airport Screener Technology Improvement Act of 2005 (H.R. 1818) which would create a Checkpoint Screening Security Fund for deploying next generation checkpoint screening technologies and would significantly increase the funding levels for the Aviation Security Capital Fund. Also, Representative Israel has introduced the Commercial Airline Missile Defense Act (H.R. 2780) which calls for equipping all air carrier passenger jets with electronic systems to protect against shoulder-fired missiles. In July 2005, Representative Sweeney introduced the General Aviation Security Act of 2005 (H.R. 3397) that would require all general aviation airports to implement specific security plans and specific security procedures that would be reviewed by the DHS every three years. **(CRS contacts: Bart Elias, Aviation; Dan Morgan, Security Technology)**

Transit and Passenger Rail Security

The bombings of transit trains and a bus in London in July 2005, like the bombings of commuter trains and subway trains in Madrid and Moscow in 2004, highlighted the vulnerability of passenger rail systems to terrorist attacks. Passenger rail 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 airline passengers undergo. Thus, transit security measures tend to emphasize managing the consequences of an attack, as opposed to preventing an attack. Nevertheless, there are prudent steps that can be taken to reduce the risks, as well as the consequences, of an attack. These include vulnerability assessments; emergency planning; emergency response training and drilling of transit personnel, ideally in coordination with police, fire, and emergency medical personnel; and communication and safety equipment. Additional options include increasing the number of transit security personnel, installing video surveillance equipment in vehicles and stations, and conducting random inspections of platforms and trains using 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.

There are no independent assessments of transit security needs and costs. The transit community has requested $5.2 billion in federal funding for security-related capital improvements, and $800 million annually in security-related operating assistance. The ability of the transit community to pay these costs themselves is limited; transit agencies run operating deficits and require government assistance just to maintain their operations. However, the average of $2.5 billion annually requested over three years is 30 times the roughly $80 million in annual transit security funding provided by Congress during FY2003-FY2005. The transit community is also requesting significant increases in non-security-related transit funding to accommodate growing demand. In light of current and projected federal deficits, federal activities potentially face constrained budgets. Given limited resources, some argue that the federal government could better enhance domestic security, at less cost, through strengthening the anti-terrorist efforts of intelligence-gathering and law-enforcement agencies rather than funding security improvements to the many potential domestic targets. **(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. One can envision a scenario where government authorities receive intelligence that a terrorist weapon or terrorists themselves are being smuggled in a particular shipment. Authorities would then want to locate that shipment immediately as well as any other possible shipments that were suspect based on having similar shipment particulars. Currently, outside the parcel industry, authorities would have limited capabilities to locate such shipments quickly. Some trucking firms have outfitted their trucks with Global Positioning System (GPS) technology. However, this capability is generally limited to large trucking firms which have a large enough fleet to make tracking equipment commercially worthwhile, in addition to having the financial resources to afford such technology. Smaller trucking firms, which carry a significant portion of freight, have not invested in this technology. Railroads have outfitted their cars with Automatic Equipment Identification (AEI) technology, but this technology only allows tracking where a reader has been installed, such as at terminals and rail yards. Thus most railcars can be tracked at certain points but not in real-time.

Most 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. A sensor or tracking device could help ensure the integrity of container shipments during these vulnerable stages. Since the September11, 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.

Imported Cargo. Of particular concern is ensuring the integrity of imported cargo. Nearly 10 million marine containers from all corners of the globe arrive at U.S. seaports annually, while 11 million truckloads and over 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. A GAO investigation found significant shortcomings with current marine container inspection procedures and made recommendations for improving them.

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.

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.

Selected Legislation in the 109th Congress. Several surface and marine cargo security measures have been introduced in the 109th Congress. H.R. 1817, the DHS Authorization Act for FY2006, would consolidate the process of background checks for the credentialing of transportation workers, modify existing marine cargo container security initiatives, and establish a risk-based prioritization of critical infrastructure. In addition to the provisions identified at the beginning of this issue brief, S. 1052 would impose a deadline of January 1, 2006 for transportation worker credentialing regulations to be issued, require performance standards for marine container seals and locks, and require a feasibility study on the creation of a port security user fee. S. 2008, the Green Lane Maritime Cargo Security Act, would offer the benefit of reduced port inspections to shippers that agreed to adopt certain security measures to protect their shipments from terrorist infiltration. S. 376, the Intermodal Shipping Container Security Act, would require the DHS to develop a strategy to ensure the security of intermodal shipping containers, whether imported, exported, or shipped domestically and requires that no less than half of all imported containers be equipped with "smart box" technology by 2007. H.R. 173 and H.R. 785 contain a provision that would establish a federal database for the reporting and collection of cargo crime data. **(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 seeks to

determine whether specified commercial drivers pose a security threat necessitating denial of the hazmat endorsement of their commercial drivers license. 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. H.R. 153 and H.R. 1109 include a provision that would require the DHS to prepare a vulnerability assessment of freight rail transportation and to identify security risks that are specific to the transportation of hazmats by rail. H.R. 153 would provide grants to address threats pertaining to the security of hazmat transportation by rail. H.R. 909 would establish a research program intended to advance security measures for hazmat transportation. SAFETEA (P.L. 109-59) which was enacted in August 2005, includes a provision intended to ensure that Mexican- and Canadian-domiciled truck drivers transporting specified hazmat loads in the United States are subject to a background check similar to that required of U.S. drivers. 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. **(CRS Contact: John Frittelli)**

CONGRESSIONAL HEARINGS, REPORTS, AND DOCUMENTS

Non-Mode Specific.

Senate Committee on Commerce, Science, and Transportation. *Proposed Reorganization of the Department of Homeland Security*, July 19, 2005.

Senate Committee on Homeland Security and Governmental Affairs. *Department of Homeland Security — Second Stage Review*, July 14, 2005.

House Committee on Homeland Security. *The Secretary's Second-Stage Review*. July 14, 2005.

House Committee on Homeland Security. Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity. *Proposed FY2006 Budget: Integrating Homeland Security Screening Operations*. March 2, 2005.

Senate Committee on Commerce, Science, and Transportation. *TSA Budget Proposal for FY2006*. February 15, 2005.

Senate Committee on Homeland Security and Governmental Affairs. *The Department of Homeland Security: The Road Ahead*. January 26, 2005.

Aviation.

House Committee on Homeland Security. Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity. *The Future of Registered Traveler*. November 3, 2005.

House Committee on Homeland Security. Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity. *Improving Management of the Aviation Screening Workforce*. July 28, 2005.

House Committee on Homeland Security. Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity. *Leveraging Technology to Improve Aviation Security - Part II*, July 19, 2005.

House Committee on Homeland Security. Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity. *Leveraging Technology to Improve Aviation Security*, July 13, 2005.

House Committee on Homeland Security. Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity. *TSA's Registered Traveler Program, Part II*. June 16, 2005.

House Committee on Homeland Security. Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity. *TSA's Registered Traveler Program*. June 9, 2005.

Senate Committee on Commerce, Science, and Transportation. *General Aviation Security and Operations*. June 9, 2005.

House Committee on Homeland Security. Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity. *TSA's Screening of Airline Pilots: Sound Security Practice or Waste of Resources*. May 13, 2005.

Senate Committee on Commerce, Science, and Transportation. *TSA Budget Proposal for FY2006*. April 26, 2005.

GAO Report GAO-05-457. *Aviation Security: Screener Training and Performance Measurement Strengthened but More Work Remains*. Released May 2, 2005.

Transit.

House Committee on Homeland Security. Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity. *The London Bombings: Protecting Civilian Targets from Terrorist Attacks - Part II*. October 20, 2005.

Senate Committee on Homeland Security and Governmental Affairs. *After the London Attacks: What Lessons Have Been Learned to Secure U.S. Transit Systems?*. September 21, 2005.

House Committee on Homeland Security. Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity. *The London Bombings: Protecting Civilian Targets from Terrorist Attacks*. September 7, 2005.

House Committee on Homeland Security. Subcommittee on Emergency Preparedness, Science, and Technology. *The London Attacks: Training to Respond in a Mass Transit Environment*. July 26, 2005.

Surface and Marine Cargo.

House Committee on Homeland Security. Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity. *Reforming HAZMAT Trucking Security.* November 1, 2005.

Senate Committee on Commerce, Science, and Transportation. *Domestic Passenger and Freight Rail Security*. October 20, 2005.

House Committee on Homeland Security. Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity. *Homeland Security Missions of the Post-9/11 Coast Guard*. June 8, 2005.

Senate Committee on Homeland Security and Governmental Affairs. *The Container Security Initiative and Customs-Trade Partnership Against Terrorism: Securing the Global Supply Chain or Trojan Horse?*. May 26, 2005.

Senate Committee on Commerce, Science, and Transportation. *Port Security*. May 17, 2005.

House Committee on Transportation and Infrastructure. Subcommittee on Highways, Transit, and Pipelines. *Background Check Process for Truckers' Hazmat Endorsements*. May 11, 2005.

House Committee on Transportation and Infrastructure. Subcommittee on Railroads. *New Technologies for Rail Safety and Security*. April 28, 2005.

House Committee on Transportation and Infrastructure. Coast Guard and Maritime Transportation Subcommittee. *Coast Guard's Deepwater Implementation*. April 20, 2005.

House Committee on Transportation and Infrastructure. Coast Guard and Maritime Transportation Subcommittee. *FY2006 Budget for the Coast Guard and Maritime Transportation Programs; H.R. 889, The Coast Guard and Maritime Transportation Act of 2005*. March 3, 2005.

Inspector General Report OIG-05-10. *Review of the Port Security Grant Program*. January 2005.

FOR ADDITIONAL READING

CRS Report RL32022, *Air Cargo Security*, by Bartholomew Elias.
CRS Report RS21920, *Detection of Explosives on Airline Passengers: Recommendation of the 9/11 Commission and Related Issues*, by Dana Shea and Daniel Morgan.
CRS Report RS22234, *Homeland Security: Protecting Airspace in the National Capital Region*, by Bart Elias.
CRS Report RL32625, *Passenger Rail Security: Overview of Issues*, by David Randall Peterman.
CRS Report RL31733, *Port and Maritime Security: Background and Issues for Congress*, by John F. Frittelli.
CRS Report RS21293, *Terrorist Nuclear Attack on Seaports: Threat and Response*, by Jonathan Medalia.
CRS Report RS21997, *Port and Maritime Security: Potential for Terrorist Nuclear Attack Using Oil Tankers*, by Jonathan Medalia.
CRS Report RS21125, *Homeland Security: Coast Guard Operations — Background and Issues for Congress*, by Ronald O'Rourke.
CRS Report RS22041, *Legal Issues Concerning State and Local Authority to Restrict the Transportation of Hazardous Materials by Rail*, by Todd B. Tatelman.
CRS Report RL32740, *Security Threat Assessments for Hazmat Drivers*, by Paul F. Rothberg.
CRS Report RL32851, *Hazardous Materials Transportation Security: Highway and Rail Modes*, by Paul F. Rothberg.
CRS Report RL33048, *Marine Security of Hazardous Chemical Cargo*, by Paul W. Parformak and John Frittelli.
CRS Report RL32073, *Liquefied Natural Gas (LNG) Infrastructure Security: Issues for Congress*, by Paul W. Parformak.
CRS Report RL32863, *Homeland Security Department: FY2006 Appropriations*, by Jennifer E. Lake and Blas Nuñez-Neto.