

CRS Report for Congress

Passenger Rail Security: Issues and Legislation in the 110th Congress

Updated January 31, 2008

David Randall Peterman
Analyst in Transportation Policy
Resources, Science, and Industry Division



Prepared for Members and
Committees of Congress

Passenger Rail Security: Issues and Legislation in the 110th Congress

Summary

Bombings of passenger trains in Europe and Asia in the last few years have demonstrated the vulnerability of passenger rail systems to terrorist attack. The number of riders and access points makes it impractical to subject all rail passengers to the type of screening airline passengers undergo. Nevertheless, steps can be taken to reduce the risks of terrorist attacks.

The 9/11 Commission called for a systematic analysis of transportation assets, the risks to those assets, and the costs and benefits of different approaches to defending those assets. The commission also called for homeland security assistance to be distributed based on these assessments of risks and vulnerabilities, rather than according to population. A comprehensive assessment of risk across all passenger rail operations has not been submitted to Congress. Most federal assistance for passenger rail security has been allocated to systems judged by the Department of Homeland Security (DHS) to be at highest risk.

The Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) did not directly address passenger rail security, but did direct DHS to create a national strategy for transportation security. This plan would identify national transportation assets, set risk-based priorities for their protection, assign responsibilities for their protection, and recommend appropriate levels and sources of funding for these efforts. DHS delivered a classified report on a “National Strategy for Transportation Security” to Congress in September 2005; this report was updated in April 2006. A security plan for the surface transportation sector was due to Congress by the end of 2006; DHS announced the plan’s release in May 2007. The Government Accountability Office has noted that this plan is only a first step, as it is only required to describe how the most critical transportation assets will be identified and how their risk will be assessed, but is not required to address how risks to transportation assets are actually being assessed or how those assets will be protected.

The Implementing Recommendations of the 9/11 Commission Act of 2007 (H.R. 1/P.L. 110-53) signed into law on August 3, 2007, included comprehensive surface transportation security legislation. This act authorized a total of \$3.5 billion for transit security and \$2.0 billion for rail security, including grant programs for which commuter rail operators, Amtrak, and state and local governments will be eligible recipients. Some funds are specifically authorized for Amtrak’s security and tunnel safety projects. The act also authorizes DHS to regulate the employee security training programs of transit and rail entities. The FY2008 DHS appropriations act (Division E of the Consolidated Appropriations Act, 2008/P.L. 110-161) provides \$47 million for surface transportation security activities, including \$22 million for rail security inspectors and dogs, and \$400 million for public transportation and railroad security assistance grants. This report will be updated.

Contents

The Relative Risks of Passenger Rail Transportation	1
Passenger Rail Security Since September 11	3
Additional Security Options	5
Risk Management	5
Issues	6
A Federal Strategy for Passenger Rail Security	6
Coordination Between Stakeholders	7
Funding	8
Training	9
The Security/Efficiency Trade-Off	10
Legislation in the 110 th Congress	11

Passenger Rail Security: Issues and Legislation in the 110th Congress

Congressional concerns over the protection of passenger rail systems are a priority in the 110th Congress. Congress greatly expanded the federal role in passenger rail security in Title XIV (the National Transit Systems Security Act of 2007) and Title XV (Surface Transportation Security) of the Implementing Recommendations of the 9/11 Commission Act of 2007 (H.R. 1/P.L. 110-53). Multiple bombings of passenger trains in India in 2006 and 2007, preceded by the bombings of London subway trains on July 7, 2005, the alleged attempt to bomb London subway trains again on July 21, 2005, and the bombing of Spanish commuter trains in 2004, provide a backdrop to Congress's efforts to reduce the risk of attacks against passenger rail operations in the United States. The 9/11 Commission characterized the federal emphasis on aviation security spending as "fight[ing] the last war," noting that "opportunities to do harm are as great, or greater, in maritime or surface transportation."¹ This report summarizes the challenges of securing passenger rail systems, options for making decisions about security funding, industry requests for funding, and passenger-rail related legislative action. It does not address the security of freight rail operations. However, since some passenger rail operations use the same track and facilities as freight rail, these topics cannot be completely separated.

The Relative Risks of Passenger Rail Transportation

Passenger rail systems have vulnerabilities that are difficult to mitigate. But the risk to passengers on these systems from terrorist attack is quite small, relative to the number of trips these systems provide daily, and travel on passenger rail systems is safer overall than the primary alternative, the automobile.

Passenger rail service takes four forms: heavy rail (e.g., subway systems like Washington D.C.'s Metro), commuter rail (e.g., Maryland's Maryland Rail Commuter, or MARC, and Virginia's Virginia Railway Express, or VRE, trains), light rail (e.g., Dallas's DART), and intercity passenger rail (Amtrak). The first three are forms of public transit, which, along with Amtrak, share certain characteristics that make them vulnerable to attack: (1) they make scheduled stops along fixed routes; (2) their operations depend on people having quick and easy access to stations and trains; (3) the number of access points, volume of ridership, and pace of operations make it impractical to subject all rail passengers to the type of screening

¹ *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, New York: W. W. Norton, 2004, p. 391.

that airline passengers undergo; and (4) the number of operators and scale of operations of all forms of passenger rail systems in the United States make it difficult to provide uniform levels of security to each and every rail system.

Congress remains concerned about rail security in part because in recent years there have been a number of attacks on passenger rail systems in other countries. The 9/11 Commission noted in its final report, “Surface transportation systems such as railroads and mass transit remain hard to protect because they are so accessible and extensive.”² With one possible exception, CRS has been unable to find a case of a terrorist attack on a passenger rail system in the United States in recent history.³ This does not mean, however, that these systems are not vulnerable to attack.

The recent attacks on passenger rail systems in other countries have resulted in hundreds of deaths. Yet in the context of millions of people riding passenger rail every day, the risk to a rail passenger of dying in any country as the result of a terrorist attack continues to be extremely small. Conversely, during the years 2003-2005, more than 80 passengers died in accidents on rail systems in the United States.⁴ Given that Americans take more than 3.5 billion trips on passenger rail systems each year, the risk of dying in a rail accident is also extremely small, but it is not zero.

The goal of a terrorist attack is not simply to kill people, but, as the name implies, to sow terror, to disrupt the social order by spreading fear and uncertainty about the future. People have died as a result of accidents on passenger rail systems, which are more common than acts of terror against such systems, but a terrorist attack would have greater shock value. One possible consequence of such an attack could be for people to switch from using rail to other modes of transportation. Switching to one likely alternative, driving, would actually raise the risk of death, due to the higher risk of accident and injury faced by drivers compared to rail passengers.⁵

In short, while rail systems and their passengers may be vulnerable to attack, the risk of attack is smaller than other risks those passengers face, including the relatively remote risk of death by accident. Perhaps more vulnerable to attack is the nation’s sense of the social order. In the aftermath of an attack, people experience fear, especially as they consider the possibility of further attacks. While government can

² *The 9/11 Commission Report*, 2004, p. 391.

³ In 1995, an Amtrak train was derailed in Arizona, resulting in the death of one Amtrak employee and injuries to 78 passengers. This act of sabotage has sometimes been characterized as a terrorist attack, but the responsible party has never been identified, so the case remains unsolved.

⁴ Commuter and intercity passenger rail: Federal Railroad Administration, *Railroad Safety Statistics 2005 Annual Report*, Table 1-3; heavy and light rail: Federal Transit Administration, *State Safety Oversight Program Annual Report for 2005*, Appendix A: Rail Transit Fatalities, 2003-2005.

⁵ One study estimated that roughly 1,600 Americans died in the year after the attacks of September 11, 2001, as a result of switching from air travel to road travel, compared to the 256 passengers who died in the four planes that were hijacked on September 11. Gerd Gigerenzer, “Out of the Frying Pan into the Fire: Behavioral Reactions to Terrorist Attacks,” *Risk Analysis*, vol. 26, no. 2, 2006, pp. 347-351.

do things to reduce the risk of an attack on passenger rail systems, such attacks cannot absolutely be prevented. If an attack on a passenger rail system were to occur, the psychological impact could be reduced by restoring a sense of normalcy as quickly as possible.⁶ This could be accomplished by, among other things, resuming passenger rail operations and apprehending the persons responsible for the attack. As Tim O'Toole, Managing Director of London's subway system, testified, "we believe our greatest defence comes from our rapid response and restoration of service, denying terrorists the chaos and fear they are seeking and thereby discouraging their return."⁷

Passenger Rail Security Since September 11

Immediately after the attacks of September 11, 2001, the Federal Transit Administration (FTA) of the U.S. Department of Transportation (DOT) conducted vulnerability assessments of the 37 largest transit agencies, and the Federal Railroad Administration (FRA) conducted security inspections of commuter railroads. Subsequently, additional assessments of the same agencies and others were performed with assistance from the Transportation Security Administration (TSA) and the Office of Grants and Training of the Department of Homeland Security (DHS). Transit agencies have used these assessments to help identify and prioritize security actions.⁸ William Millar, president of the American Public Transportation Association (APTA), testified in January 2007 that the transit industry has spent \$2.5 billion since September 11, 2001, on security and emergency preparedness measures.⁹

In the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458), Congress directed DHS to prepare a national strategy for transportation security and security plans for each transportation mode. The national strategy was completed in 2005; the mode-specific security plans were released in May 2007. Congress has provided a total of \$1.09 billion for grants to passenger rail systems since September 11, 2001, mostly through DHS annual appropriations acts. These funds can be used for security-related planning, acquisition of equipment, training, exercises, and administrative expenses.

⁶ Todd Litman, "Terrorism, Transit and Public Safety: Evaluating the Risks," *Journal of Public Transport*, v. 8, no. 4 (2005).

⁷ Testimony of Tim O'Toole, Managing Director of London Underground, Transport for London, before the United States Senate Committee on Banking, Housing and Urban Affairs, Hearing on Transit Security, January 18, 2007.

⁸ GAO, *Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts*, GAO-05-851, September 2005, pp. 23-25.

⁹ Testimony of William W. Millar, President, American Public Transportation Association, before the Senate Committee on Banking, Housing, and Urban Affairs, January 18, 2007, p. 1.

On May 20, 2004, after the bombings of commuter trains in Madrid, TSA issued security directives for U.S. passenger rail systems.¹⁰ Although these directives were not made public, they reportedly reflected actions already taken by many U.S. rail systems.¹¹ These included removing or hardening trash containers on boarding platforms that could be used to hide bombs, increasing the presence of security officers, using video surveillance in and around stations, conducting random inspections of passengers and baggage (sometimes with the help of bomb-sniffing dogs), and encouraging riders to look for suspicious activity.¹²

The Government Accountability Office (GAO) has noted that “the issuance of these directives was an effort to take swift action in response to a current threat.”¹³ However, the GAO goes on to write that because the rail industry and federal stakeholders were afforded only limited input and review, the directives “may not provide the industry with baseline security standards based on industry best practices.”¹⁴ Furthermore, GAO “recommended that TSA collaborate with the Department of Transportation and the passenger rail industry to develop rail security standards that reflect industry best practices and that can be measured, monitored, and enforced.”¹⁵ The FRA and the passenger rail industry have raised concerns about some of these directives, including at least one that seems to conflict with other federal safety regulations.¹⁶ According to GAO, “in January 2007, TSA stated that it recognizes the need to closely partner with the passenger rail industry to develop security standards and directives.”¹⁷

Since September 2005, TSA has hired 100 surface transportation inspectors to monitor and enforce compliance with TSA rail security directives. In September 2006, FRA’s and TSA’s roles and responsibilities for compliance inspections were outlined in an annex to the existing memorandum of understanding between DHS

¹⁰ United States Department of Homeland Security Press Office, “Department of Homeland Security Announces New Measures to Expand Security for Rail Passengers,” May 20, 2004.

¹¹ Peter Whoriskey, “U.S. Issues Anti-Terror Regulations for Rail Systems,” *Washington Post*, May 21, 2004, p. B1.

¹² See “Table 1: Examples of Measures Required by TSA Security Directives Issued to Passenger Rail Operators and Amtrak,” in Government Accountability Office, *Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts*, GAO-06-181T, October 20, 2005, p. 22.

¹³ Government Accountability Office, *Homeland Security: Progress Has Been Made to Address the Vulnerabilities Exposed by 9/11, but Continued Federal Action Is Needed to Further Mitigate Security Risks*, GAO-07-375, January 2007, pp. 52-53.

¹⁴ *Ibid.*, p. 53.

¹⁵ *Ibid.*

¹⁶ FRA safety regulations (49 U.S.C. § 114(1)) require that engineer compartment doors be unlocked to aid emergency escapes, but one of the TSA security directives requires that doors equipped with locking mechanisms be kept locked. Government Accountability Office, *Passenger Rail Security: Federal Strategy and Enhanced Coordination Needed to Prioritize and Guide Security Efforts*, GAO-07-442T, February 6, 2007, p. 16.

¹⁷ *Ibid.*

and DOT. Additionally, according to TSA, their “inspectors have developed relationships with security officials in passenger rail and transit systems, coordinated access to operations centers, participated in emergency exercises, and provided assistance in enhancing security.”¹⁸

Additional Security Options

In studying the security measures taken by U.S. and some foreign transit agencies, GAO found that the domestic and foreign agencies were doing many of the same things.¹⁹ But GAO identified three practices used by a limited number of nations that are not currently in general use in the United States. These are (1) covert testing of employee response to incidents by placing suspicious items throughout the system or setting off alarms, (2) random screening of passengers and baggage, and (3) a national government clearinghouse of security technologies and best practices.²⁰ GAO noted that attempts to implement these three practices in the U.S. could face political, legal, fiscal, and cultural challenges.²¹ GAO also identified government centralization of the process for researching and developing passenger rail security technologies as a potentially useful practice. GAO found that no U.S. federal agency has collected or distributed information on research and development of passenger rail security technologies, or other best practices for passenger rail security.²²

Risk Management

TSA is using a risk-based methodology to guide its security efforts.²³ GAO²⁴ and the 9/11 Commission²⁵ recommended the use of a risk-based methodology to guide security actions, and the Homeland Security Act of 2002 (P.L. 107-296) directed that this approach be used for protecting key resources and critical infrastructure assets.

¹⁸ Ibid.

¹⁹ GAO, *Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts*, GAO-07-225T, January 18, 2007, pp. 18-25.

²⁰ Only 2 of the 13 foreign systems GAO studied were using covert testing, and only 2 of the 13 were randomly screening passengers and their baggage, at the time of GAO’s study.

²¹ New York’s police department was sued over its conducting of random voluntary searches at subway station entrances, but it won the case. Alan Feuer, “Appeals Court Upholds Random Police Searches of Passengers’ Bags on Subways,” *New York Times*, August 12, 2006, p. B5.

²² GAO-07-225T, p. 24.

²³ Kip Hawley, Assistant Secretary, Transportation Security Administration, Department of Homeland Security, Testimony before the House Committee on Homeland Security, Subcommittee on Transportation Security and Infrastructure Protection, February 6, 2007.

²⁴ *Transportation Security: Federal Action Needed to Help Address Security Challenges*, GAO-03-843, June 2003, p. 51.

²⁵ *The 9/11 Commission Report*, pp. 391, 396.

Threat-based risk management includes three components: vulnerability, threat, and criticality (or consequence).²⁶ ‘Vulnerability’ encompasses the ways a system may be open to attack; ‘threat’ considers the likelihood of an attack on a system; and ‘criticality’ refers to the potential consequences of an attack. The assessment of the level of risk results from the interplay of these components.

One implication of risk analysis is that there is more than one way to manage risk to a passenger rail system. Specific strategies can be tailored to specific rail systems by combining one or more of the following approaches. One approach is to make changes in passenger rail systems to lower their vulnerability to attack (e.g., hiring more police officers, introducing random screening of passengers and bags, installing security cameras). Another is to reduce the potential consequences of an attack (e.g., through coordinated emergency response training exercises with local first responders). Yet another is to make changes elsewhere that reduce the level of threat to those systems (e.g., putting more money into intelligence and law enforcement to combat terrorism).

Issues

A Federal Strategy for Passenger Rail Security. In the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458), Congress directed DHS, working jointly with DOT, to prepare a strategy for transportation security, with plans for each mode of transportation. This strategic plan is to include “risk-based priorities across all transportation modes” for protecting transportation assets, “the most appropriate, practical, and cost-effective means of defending those assets,” and “the agreed upon roles and missions of Federal, state, regional, and local authorities.” Such plans would provide guidance to federal agencies and other stakeholders as to the goals, objectives, roles and responsibilities for passenger-rail related security activities.

This national transportation strategic plan, and the security plans for each transportation mode, were due to Congress by April 1, 2005. Due to the sensitive nature of some of this information, the act provided that classified information shall be provided to the appropriate congressional committees separately. DHS sent a classified report to Congress in September 2005 on a “National Strategy for Transportation Security.”²⁷ The release of the mode-specific security plans was

²⁶ For more discussion of risk management, see CRS Report RL32561, *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threat, Vulnerabilities and Consequences*, by John Moteff; and Carl A. Roper, *Risk Management for Security Professionals*, Butterworth-Heinemann, 1999. GAO reported that DHS used a variant of this approach, where “Criticality” referred to critical assets that enable the operator to achieve its mission, and “Impact” measures the consequence of an attack on critical assets. GAO, *Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts*, GAO-05-851, September 2005, pps. 21-22.

²⁷ *Detour Ahead: Critical Vulnerabilities in America’s Rail and Mass Transit Security Programs*, prepared at the request of Congressman Bennie G. Thompson, ranking Member, by the Democratic Staff of the Committee on Homeland Security, United States House of (continued...)

announced by DHS on May 21, 2007, as part of an announcement of the completion of all seventeen sector-specific infrastructure sector plans discussed below.²⁸ TSA has testified that the mode-specific plans identify underwater and underground tunnels in as one of the highest security priorities.

In 2006, DHS also issued a National Infrastructure Protection Plan (NIPP) to serve as a guide to using risk management principles for prioritizing protection efforts within infrastructure sectors (e.g., transportation) and across sectors.²⁹ The NIPP required that sector-specific agencies submit plans to DHS by December 2006 identifying critical assets, evaluating the risk to them, and developing measures to protect them. The NIPP called for the sector plans to be developed by councils of federal, state, and regional and local government agencies involved in that sector, along with sector councils made up of private sector stakeholders. The government council for the transportation sector was formed in January 2006, but, alone among the seventeen infrastructure sectors, the transportation sector did not have a private sector council as of March 2007, though reportedly each transportation mode has a sector council.³⁰ DHS indicates that “once the modes are organized,” an overall transportation sector council will be formed.³¹ DHS announced that the transportation sector-specific plan (along with the other sector plans) and transportation mode-specific annexes were completed on May 21, 2007. GAO notes 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.”³²

Coordination Between Stakeholders. TSA is the agency primarily responsible for transportation security. It was originally created within the DOT, but was transferred to DHS when that department was created. DOT agencies remain responsible for safety within transportation modes, a responsibility that often overlaps with security. The passenger rail industry has raised concerns about TSA’s degree of understanding of their industry, and openness, compared with DOT agencies such as the FRA and FTA, with whom the industry has long-established

²⁷ (...continued)

Representatives, (no date, approximately June 2006), p. 17. The initial version of the National Strategy for Transportation Security was criticized by the original 9/11 Commission members, acting as a private organization called the “9/11 Public Discourse Project,” as lacking “the necessary detail to make it an effective management tool.” 9/11 Public Discourse Project, *Final Report on 9/11 Commission Recommendations*, December 5, 2005. Available at [http://www.9-11pdp.org/press/2005-12-05_report.pdf] (viewed November 29, 2006).

²⁸ Unrestricted access versions of the transportation sector plan, and the mode-specific plans, are available at [http://www.dhs.gov/xprevprot/programs/gc_1179866197607.shtm].

²⁹ Government Accountability Office, *Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors’ Characteristics*, GAO-07-39, October 16, 2006, p. 2-3.

³⁰ Government Accountability Office, *Critical Infrastructure: Challenges Remain in Protecting Key Sectors*, GAO-07-626T, March 20, 2007, p. 3.

³¹ *Ibid*, p. 11.

³² transportation *Ibid*, p. 5.

ties. For example, as noted above, passenger rail operators have reported that TSA did not adequately consult with the industry in developing the directives for passenger rail security, and concerns have been raised about some of the directives conflicting with other passenger rail industry regulations. GAO noted that TSA has recently said it recognizes the need to work more closely with the passenger rail industry in developing security standards and directives.³³ To improve coordination between DHS and DOT in transportation security, they have signed a Memorandum of Understanding defining their responsibilities and procedures for cooperation. TSA has signed annexes — more specific agreements focusing on individual transportation modes and other matters — with FTA and FRA.

Funding. In the absence of plans that would allow Congress to consider the risks to individual passenger rail systems and across the passenger rail sector, and the costs of addressing those risks; Congress provided \$690 million from FY2003-FY2007 for security grants to all passenger rail (and some other) transit agencies and Amtrak; for FY2008, Congress increased the amount provided annually for these grants significantly, to \$400 million.³⁴

The passenger rail and transit communities have made security improvements, but say they are constrained by the limits of available funding. They assert that their primary security issue is finding a way to pay for additional security improvements. As noted earlier, William Millar, president of APTA, has testified that the transit industry (which includes bus-only systems as well as rail systems, but does not include Amtrak) has spent over \$2.5 billion on security activities since 9/11.³⁵ In a 2004 survey, APTA members (transit-system operators) were asked, “How much additional funding do you need in the long-term to complete your capital program to maintain, modernize, and expand your security function?”³⁶ Based on survey responses, APTA estimates that there are over \$6 billion in unmet long-term security needs: \$5.2 billion in security-related capital investment (for protection of infrastructure and vehicles, enhancing evacuation capabilities, and improving emergency response) and \$800 million annually in ongoing operating and

³³ Government Accountability Office, *Passenger Rail Security: Federal Strategy and Enhanced Coordination Needed to Prioritize and Guide Security Efforts*, GAO-07-583T, March 7, 2007, p. 14.

³⁴ These funds were provided in DHS annual appropriations acts, except for \$100 million that was provided through the U.S. Troop Readiness, Veterans’ Care, Katrina Recovery, and Iraq Accountability Appropriations Act, 2007 (P.L. 110-28). Since FY2005, freight rail companies have also been eligible for these grants. In addition, Congress made one-time appropriations of \$100 million to Amtrak and \$39 million to the Washington Metropolitan Area Transit Authority for security expenses in the FY2002 Department of Defense Appropriations Act (P.L. 107-117).

³⁵ Greg Hull, Director of Operations, Safety and Security Programs, American Public Transportation Association, Testimony before the House Committee on Appropriations Subcommittee on Homeland Security, February 13, 2007.

³⁶ American Public Transportation Association, *Survey of United States Transit System Security Needs and Funding Priorities: Summary of Findings*, April 2004, p. 11.

maintenance expenditures.³⁷ APTA has repeatedly requested significant increases in federal grants to help pay for those security improvements.

Funding security improvements for passenger rail has been primarily a state and local responsibility. Advocates of greater federal responsibility for security funding argue that, since the current concern is chiefly about attacks from terrorists, the federal government should bear more responsibility for providing security funding, reflecting its role of providing for the national defense.

Advocates for a more limited federal role in funding passenger rail security improvements argue that the federal government is exercising its national defense responsibility through funding national defense efforts and that taxpayers all over the country should not be required to pay for security improvements for a relatively small number of transit agencies located in large metropolitan areas. They note that comparisons with the level of federal spending for aviation security are not necessarily apt, in part because a significant portion of the federal spending for aviation security is funded through fees assessed on airline passengers.

Many of the security measures that passenger rail organizations may employ have other benefits to those systems, often in reducing other types of threat to passengers (for example, from ordinary criminal activity and accidents) that are considered to be chiefly local responsibilities. In addition to the grants provided specifically for passenger rail security, the federal government has provided billions of dollars to state and local governments through the broader Urbanized Areas Security Initiative for security-related activities, funds which the state and local governments have the discretion to apply to those activities they judge as having the greatest security value to their communities.

The National Transit Systems Security Act of 2007 (Title XIV of P.L. 110-53), enacted on August 3, 2007, authorized a total of \$2.6 billion for grants for security-related capital expenses and \$840 million for grants for security-related operating expenses over a four-year period (FY2008-FY2011). These are authorizations for funding; the actual amounts to be provided are still to be determined by Congress each year through appropriations for DHS. Given constrained federal budgets and the many competing demands for funding, the argument over the appropriate size of the federal role in funding passenger rail and transit security improvements may continue to be heard during the annual appropriations process.

Training. Training of employees — including training in what to look for and practice drills in how to respond to an attack — has been identified as the most important component in a passenger rail system's security plan.³⁸ Training courses

³⁷ Ibid. This estimate is for the entire transit industry, not just passenger rail operators. Most transit agencies only provide bus service, but the largest transit agencies also operate rail systems, and rail systems represent the bulk of transit infrastructure.

³⁸ Testimony of Tim O'Toole, Managing Director of Transport, City of London, Before the Committee on Banking, Housing, and Urban Affairs, United States Senate, Hearing on Examining the State of Transit Security, January 18, 2007; Kip Hawley, Deputy (continued...)

have been developed and provided by the federal government. Further development of these training courses is ongoing. Representatives of rail labor have questioned the effectiveness of this training and the extent to which it has been provided to employees. They have cited FTA testimony in the fall of 2006 to the effect that fewer than a quarter of the nation's transit employees had received security training.³⁹ TSA has testified that the security skills needed by transit employees can be acquired through "extensive training, rigorous emergency planning, and regular emergency testing and drills," and has acknowledged that they, and the transit industry, need to provide more training for more employees.⁴⁰ Such training can be costly, especially drills, since operators need to keep their systems running while their employees receive training or participate in drills. The National Transit Systems Security Act of 2007 (Title XIV of P.L. 110-53) authorizes funding for grants to transit and rail operators to provide security training for their employees; the amount of funding to be provided for those grants will be determined by Congress each year through appropriations to DHS. The act also authorizes DHS to regulate the security training programs of transit and rail operators.

The Security/Efficiency Trade-Off. One key policy issue for passenger rail is the trade-off between security and efficiency. Few would argue that passenger rail could ever be made invulnerable to attack. Also, there appears to be general agreement that there are other federal security priorities beyond passenger rail. Some observers, noting that the number of potential terrorist targets in the United States — such as passenger trains and stations, buses, schools, shopping malls, sporting events, etc. — is virtually limitless, question the value of efforts to make each of these targets more secure. They argue that many such efforts are not cost-effective, given that if one set of targets — for example, trains — is made more secure, terrorists might simply shift to softer targets such as buses or shopping malls. Attacks on these targets could plausibly have a similar impact to an attack on a passenger train or subway. Moreover, these security efforts impose a variety of costs on the public, in money, time, inconvenience, and limitations on personal freedoms.

³⁸ (...continued)

Administrator, Transportation Security Administration, also described training of employees (and awareness of passengers) as TSA's number one priority in response to a question from Representative DeFazio, House Committee on Homeland Security, Subcommittee on Transportation Security and Infrastructure Protection, February 6, 2007. In APTA's 2004 transit security survey, training was identified as the second most important issue, behind funding current transit agency/local law enforcement security personnel. APTA. *Survey of United States Transit System Security Needs and Funding Priorities*, pp. 12-13.

³⁹ Testimony of Warren S. George, International President, Amalgamated Transit Union, Before the United States Senate Committee on Banking, Housing, and Urban Affairs, "Examining the State of Transit Security," January 18, 2007, p. 9-10. FTA had testified in the fall of 2006 that 80,000 transit workers had received training; there are an estimated 400,000 transit employees.

⁴⁰ Testimony of John P. Sammon, Assistant Administrator for Transportation Sector Network Management, Transportation Security Administration, United States Department of Homeland Security, before the United States House of Representatives Committee on Homeland Security, Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity, Hearing on Transit Security Training Procedures, September 28, 2006, p. 2.

Some observers argue that a more effective strategy is to increase efforts to disrupt the terrorist groups that are the source of these threats (e.g., funding for intelligence and law enforcement agencies), and efforts to respond to an attack (e.g., funding for first responders).⁴¹ Also, efforts to prepare transportation systems to resume operations quickly after an incident — referred to as the resiliency of the system — is also seen by some observers as more valuable than efforts to further secure inherently vulnerable systems, especially those systems that are not at the greatest risk or those assets that are not the most critical to a system.⁴²

Legislation in the 110th Congress

Congress passed comprehensive passenger rail security legislation as part of the Implementing Recommendations of the 9/11 Commission Act of 2007 (H.R. 1), which was signed into law August 3, 2007 (P.L. 110-53). Titles XIV (the National Transit Systems Security Act of 2007) and Title XV (Surface Transportation Security) of this legislation expand the federal role in securing passenger rail, both by authorizing significant increases in federal grants to passenger rail operators for security improvements and by authorizing federal regulation of certain security-related activities of transit and rail operators, such as employee training.

Passenger rail security-related provisions in the legislation include authorization for several new grant programs: a total of \$3.4 billion over the period FY2008-FY2011 for grants for public transportation security, for which commuter rail agencies will be among the eligible recipients (§ 1406); a total of \$1.2 billion over the same period for grants for railroad security, for which eligible recipients include rail carriers, Amtrak, and state and local governments (§ 1513); a total of \$650 million over the same period for grants to Amtrak for systemwide security upgrades (§ 1514); and a total of \$200 million over the same period for grants to Amtrak for safety improvements to rail tunnels in New York, Baltimore, and Washington, DC (§ 1515). These grants are to be administered by DHS, except that the Amtrak systemwide security grants are to be awarded by DHS but disbursed by DOT, and the Amtrak tunnel safety grants are to be administered by DOT.

Of the \$3.4 billion authorized for the public transportation grant program, \$840 million can be used for security-related operating expenses (e.g., employee training, canine patrols); the remaining \$2.56 billion is for security-related capital projects (e.g., tunnel and perimeter protection, communications equipment, surveillance equipment). These transit security grants will go directly to transit agencies, in contrast to the transit security grant program DHS has been administering, under

⁴¹ Jennifer Barrett, “An Enormous Waste of Money: Interview with Security Expert Bruce Schneier,” *Newsweek* Web Exclusive, March 17, 2004 [<http://www.msnbc.msn.com/id/4549661/>], viewed July 8, 2004. Kip Hawley, Assistant Secretary of TSA, recently testified that “the best defense is one that prevents the terrorists from ever entering the United States.” Testimony before the United States House of Representatives Committee on Homeland Security, Hearing on Rail and Surface Transportation Security, March 6, 2007, p. 2.

⁴² Government Accountability Office, *Critical Infrastructure: Challenges Remain in Protecting Key Sectors*, GAO-07-626T, March 20, 2007, p. 18-19.

which the grants go to a state's security coordinating agency. No local match will be required for these grants, though the act directs DHS to study the feasibility of establishing surface (and maritime) transportation-related user fees as a dedicated revenue source for funding security improvements (§ 1308).

Other provisions of the legislation include an authorization of \$100 million for transit security research and development (§ 1409); an authorization of \$132 million for rail security related research and development (§ 1518); a requirement that public transportation agencies (§ 1405) and railroads (§ 1512) considered to be high-risk targets by DHS must have security plans that have been approved by DHS; authorization for funding for TSA to hire up to 100 more surface transportation security inspectors (currently TSA has 100 such inspectors) (§ 1304); a requirement that DHS conduct a name-based security background check and an immigration status check on all public transportation (§ 1411) and railroad (§ 1520) frontline employees; and authority for DHS to regulate transit (§ 1408) and rail (§ 1517) employee security training standards.

Legislation dealing with appropriations for the Department of Homeland Security also has implications for passenger rail security. The FY2008 DHS appropriations act (Division E of the Consolidated Appropriations Act, 2008/P.L. 110-161) provided \$47 million for surface transportation security activities (up from \$37 million in FY2007), including \$22 million for rail security inspectors and canine teams (up from \$13 million in FY2007), and \$400 million for public transportation and railroad security assistance grants (up from \$275 million⁴³ in FY2007).

⁴³ Congress provided \$175 million for this grant program as part of DHS's annual appropriation in the Revised Continuing Appropriations Resolution, 2007 (P.L. 110-5), signed into law on February 15, 2007, and another \$100 million for the program through the U.S. Troop Readiness, Veterans' Care, Katrina Recovery, and Iraq Accountability Appropriations Act, 2007 (P.L. 110-28), signed into law on May 5, 2007.