United States Government Accountability Office

GAO

Report to Congressional Requesters

September 2005

PASSENGER RAIL SECURITY

Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts

GAO
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-05-851, a report to congressional requesters

September 2005

PASSENGER RAIL SECURITY

Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts

Why GAO Did This Study

The U.S. passenger rail system is a vital component of the nation's transportation infrastructure, carrying more than 11 million passengers each weekday. The Department of Homeland Security (DHS) and the Department of Transportation (DOT) share responsibility for ensuring the safety and security of rail systems.

In this report, GAO addressed (1) DHS actions to assess the risks to the U.S. passenger rail system in the context of prevailing risk management principles, (2) federal actions taken to enhance the security of the U.S. passenger rail system, and (3) security practices that domestic and selected foreign passenger rail operators have implemented.

What GAO Recommends

GAO is recommending, among other things, that the Secretary of DHS direct the Assistant Secretary of the Transportation Security Administration (TSA) to develop a plan with timelines for completing its methodology for conducting risk assessments and develop rail security standards that can be measured and enforced. The Secretary also should consider the feasibility of implementing certain security practices used by foreign operators. DHS, DOT, and Amtrak reviewed a draft of this report and generally agreed with the report's recommendations. DHS's detailed comments and GAO's response are contained in the report.

www.gao.gov/cgi-bin/getrpt?GAO-05-851.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Cathleen Berrick at (202) 512-8777 or JayEtta Hecker at (202) 512-2834

What GAO Found

Within DHS, the Office for Domestic Preparedness has completed 7 risk assessments of passenger rail systems around the country, with 12 more under way. TSA has begun to conduct risk assessments and to establish a methodology for determining how to analyze and characterize risks that have been identified but has not yet completed either effort or set timelines for doing so. TSA will not be able to prioritize passenger rail assets and help guide security investment decisions until these efforts are completed. At the department level, DHS has begun developing, but has not yet completed, a framework to help agencies and the private sector develop a consistent approach for analyzing and comparing risks to transportation and other sectors. Until this framework is finalized and shared with stakeholders, it may not be possible to compare risks across different sectors, prioritize them, and allocate resources accordingly.

The Federal Transit Administration and Federal Railroad Administration within DOT have ongoing initiatives to enhance passenger rail security. In addition, in 2004, TSA issued emergency security directives to domestic rail operators after terrorist attacks on the rail system in Madrid, Spain, and piloted a test of explosive detection technology for use in passenger rail systems. However, federal and rail industry officials raised questions about the feasibility of implementing and complying with the directives, citing limited opportunities to collaborate with TSA to ensure that industry best practices were incorporated. In September 2004, DHS and DOT signed a memorandum of understanding to improve coordination between the two agencies, and they are developing agreements to address specific rail security issues.

Domestic and foreign passenger rail operators we contacted have taken a range of actions to help secure their systems. We also observed security practices among certain foreign passenger rail systems or their governments that are not currently used by the domestic rail operators we contacted, or by the U.S. government, and which could be considered for use in the United States. For example, some foreign rail operators randomly screen passengers, and some foreign governments maintain centralized clearinghouses on rail security technologies and best practices.

Example of high visibility canine sweep at mass transit station

Source: Developed by GAO with photo provided by Washington Metropolitan Area Transit Authority.

Contents

Tables

Figures

Abbreviations

AAR	American Association of Railroads
APTA	American Public Transportation Association
ATSA	Aviation and Transportation Security Act
BART	San Francisco Bay Area Rapid Transit
CCTV	closed-circuit television
DHS	Department of Homeland Security
DOT	Department of Transportation
FRA	Federal Railroad Administration
FTA	Federal Transit Administration
HSPD-7	Homeland Security Presidential Directive-7
IAIP	Information Analysis and Infrastructure Protection
MBTA	Massachusetts Bay Transportation Authority
MOU	memorandum of understanding
NIPP	National Infrastructure Protection Plan
ODP	Office for Domestic Preparedness
PANYNJ	Port Authority of New York and New Jersey
PATH	Port Authority Trans-Hudson
PDA	personal digital assistant
RATP	Regie Autonome des Transports Parisiens
SLGCP	Office of State and Local Government Coordination and Preparedness
TRIP	Transit and Rail Inspection Pilot
TSA	Transportation Security Administration
TSSP	transportation sector-specific plan
UASI	Urban Area Security Initiative
WMATA	Washington Metropolitan Area Transit Authority

G A O
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

September 9, 2005

The Honorable Steven LaTourette
Chairman
Subcommittee on Railroads
Committee on Transportation and Infrastructure
House of Representatives

The Honorable Olympia Snowe
United States Senate

The Honorable Barbara Boxer
United States Senate

The Honorable Michael Castle
House of Representatives

The July 7 and July 21, 2005, bomb attacks on London's subway system, which resulted in over 50 fatalities and more than 700 injuries, dramatically highlighted the vulnerability of passenger rail systems worldwide to terrorist attacks and the need for an increased focus on security for these systems. The U.S. passenger rail system is a vital component of the nation's transportation infrastructure, encompassing rail transit (heavy rail, commuter rail, and light rail) and intercity rail systems.[1] Together, these systems carry more than 11 million passengers each weekday. One of the critical challenges facing rail system operators—and the federal agencies that regulate and oversee them—is finding ways to protect rail systems from potential terrorist attacks without compromising the accessibility and efficiency of rail travel.

[1] The U.S. passenger rail system consists of heavy, commuter, light, and intercity rail systems. Heavy rail is an electric railway that can carry a heavy volume of traffic. Heavy rail is characterized by high speed and rapid acceleration, passenger rail cars operating singly or in multi-car trains on fixed rails, separate rights of way from which all other vehicular and foot traffic is excluded, sophisticated signaling, and high-platform loading. Most subway systems are considered heavy rail. Commuter rail is characterized by passenger trains operating on railroad tracks and providing regional service, such as between a central city and its adjacent suburbs. Light rail systems typically operate passenger rail cars singly (or in short, usually two-car, trains) and are driven electrically with power being drawn from an overhead electric line. Amtrak operates the nation's primary intercity rail system.

Several entities play a role in helping to fund and secure the passenger rail industry. The Department of Homeland Security's (DHS) Transportation Security Administration (TSA) is the primary regulator of the rail system's security, while DHS's Office for Domestic Preparedness (ODP) has been the primary federal source of security funding for passenger rail systems. In addition, the Department of Transportation's (DOT) Federal Transit Administration (FTA) and Federal Railroad Administration (FRA), state and local agencies (which operate most rail transit rail systems), and Amtrak are responsible for or have been involved in the security and safety of the U.S. passenger rail system.

In the United States, passenger rail systems represent one of many modes of transportation—along with aviation, maritime, and others—competing for limited federal security resources. Within the passenger rail sector itself, there is competition for resources, as federal, state, and local agencies and rail operators seek to identify and invest in appropriate security measures to safeguard these systems while also investing in other capital and operational improvements. Moreover, given competing priorities and limited homeland security resources, difficult policy decisions have to be made by Congress and the executive branch to prioritize security efforts and direct resources to areas of greatest risk within the passenger rail system, among all transportation modes, and across other nationally critical sectors.

In this regard, to help federal decision makers determine how to best allocate limited resources, we have advocated, the National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission) has recommended, and the subsequent Intelligence Reform and Terrorism Prevention Act of 2004 requires, that a risk management approach be employed to guide security decision making. [2] A risk management approach entails a continuous process of managing risks through a series of actions, including setting strategic goals and objectives, assessing and quantifying risks, evaluating alternative security measures, selecting which measures to undertake, and implementing and monitoring those measures. In July 2005, in announcing his proposal for the reorganization of DHS, the Secretary of the Department of Homeland Security declared that as a core principle of the reorganization, the department must base its work on priorities driven by risk.

[2] Pub. L. No. 108-458, 118 Stat. 3638.

You have expressed interest in the progress federal agencies and domestic passenger rail operators have made in setting and implementing security priorities in the wake of September 11 and terrorist attacks on rail systems. In addition, you expressed interest in learning about the security practices implemented by foreign passenger rail operators. For this report, we analyzed (1) the actions that DHS and its component agencies have taken to assess the risks posed by terrorism to the U.S. passenger rail system in the context of prevailing risk management principles; (2) the actions that federal agencies have taken to enhance the security of the U.S. passenger rail system; and (3) the security practices that domestic and selected foreign passenger rail operators have implemented to mitigate risks and enhance security, and any differences in these practices.

To perform our analyses, we conducted site visits at, or held teleconferences with, a total of 32 passenger rail operators in the United States that represent over 95 percent of the nation's total rail ridership, as well as Amtrak. We also conducted site visits or met elsewhere with 13 passenger rail operators in seven European and Asian countries. During our domestic and international visits, we interviewed management and security personnel, toured stations and other facilities such as control centers, observed security practices, and obtained documentation of security procedures. In addition, we interviewed officials from domestic and foreign rail industry associations, foreign governments and rail operators, and representatives of the European Commission. Because we selected a nonprobability sample of both foreign and domestic passenger rail operators, the information we obtained from these interviews and visits cannot be generalized to all foreign or domestic rail operators.

We also reviewed risk assessments of U.S. rail systems conducted by the federal government. Risk assessments are used to identify and rank risks to critical regional or national assets to further identify which would be most vulnerable to attack based on various threat scenarios. Risk assessments are an integral part of using a broader risk management approach to guide investments that help enhance security. While a risk management approach entails multiple iterative components, this report primarily addresses the risk assessment component of such an approach as applied in the homeland security context. (Additional information about the risk assessment component is contained in app. II.) Although we identified and cataloged security practices of the domestic and foreign passenger rail operators we contacted, we did not evaluate the appropriateness or effectiveness of these practices. We discussed foreign security practices we observed with DHS, DOT, passenger rail industry associations, select passenger rail operators, and transportation security experts from the RAND Corporation and the Mineta Transportation Institute to explore the potential applicability of these practices to U.S. passenger rail systems.[3] Our work does not reflect the proposed reorganization of DHS and its component agencies announced by the Secretary of DHS. We conducted our work from May 2004 through July 2005 in accordance with generally accepted government auditing standards. Appendix I contains more details about our objectives, scope, and methodology.

Results in Brief

Two component agencies with different missions within DHS are responsible for, and have engaged in, conducting risk assessments for the passenger rail industry, in an effort to identify and protect the assets most vulnerable to attack and most critical to operations, such as stations, tracks, and bridges. The first, the Office for Domestic Preparedness, is responsible for, among other things, providing grant funds and technical assistance to rail operators and others to improve preparedness at the state and local level. As part of this mission, ODP has developed and implemented a risk assessment methodology for mass transit agencies and port authorities, and used it to complete 7 risk assessments at rail facilities, with an additional 12 assessments in progress, as of July 2005. According to passenger rail operators we interviewed, ODP's risk management approach has helped them to prioritize and allocate resources to protect their systems. For example, one operator collaborated with ODP on a risk assessment that resulted in justifying a $500 million high-priority security capital investment program, which is to fund, among other things, a security operations center for its passenger train network, alarm monitoring systems, and an upgraded closed-circuit television system. The second agency, TSA, has also recently begun to conduct risk assessments of the rail sector as part of a broader effort to assess risk to all transportation modes. As of July 2005, while TSA had completed an overall threat assessment for mass transit and passenger rail, the agency had not yet completed a risk assessment for the passenger rail sector or a methodology for determining how to analyze and characterize risk (as high, medium, or low) identified through assessments, or indicated when this would be done. Until both of these efforts have been accomplished, in collaboration with rail industry stakeholders, TSA will not be able to prioritize passenger rail assets based

[3] The institute was established by Congress as part of the Intermodal Surface Transportation Efficiency Act of 1991 and focuses on international surface transportation policy issues involving research, education, and technology transfer. RAND is a nonprofit research organization that analyzes security issues in the rail sector, among other things.

on risk and help guide investment decisions about protecting them. A 2003 presidential directive required DHS to, among other things, establish uniform guidelines and methodologies for integrating federal infrastructure protection and risk management activities within and across entire economic sectors, such as transportation (including rail), energy, and agriculture. To address this requirement, at the department level, DHS has been developing a broad framework intended to help federal agencies, the private sector, and state and local governments develop a consistent approach to analyzing risk to critical infrastructure within and across sectors. This framework is intended to enable risks across sectors to be compared as a means of guiding resource allocation and emergency response planning. Because DHS has not yet finalized this framework, it is not known what impact, if any, it may have on risk assessment efforts now under way by TSA, ODP, and other federal agencies with critical infrastructure protection responsibilities. Until DHS finalizes this framework, it may not be possible to compare risks across different sectors, prioritize them, and then allocate resources accordingly.

A number of federal departments and their component agencies have taken actions to strengthen passenger rail security. FTA and FRA were the primary federal agencies involved in passenger rail security matters prior to the creation of TSA, and both undertook numerous initiatives both before and after September 11, 2001. For example, FTA conducted security readiness assessments, sponsored security training, and developed security guidance for transit agencies. FRA conducted security inspections of commuter railroads and researched various rail security technologies. After taking over as the lead federal agency responsible for transportation security, TSA issued security directives to the passenger rail industry in May 2004, after terrorists attacked the commuter rail system in Madrid, Spain. The directives—based upon industry best practices, according to TSA—required rail operators to implement a number of security measures, such as conducting frequent inspections of stations, terminals, and other assets, or utilizing canine explosive detection teams, if available. According to TSA officials, because of the need to act quickly, the rule-making process for these security directives did not include a public comment period. As a result, stakeholder input was limited. The rapid issuance of these directives has posed challenges to TSA and rail operators. For example, while rail operators are required to implement the measures, and TSA has hired rail inspectors to enforce them, operators told TSA they were unsure how to comply with the directives because, for example, the directives include instructions requiring them to perform "frequent inspections" of key facilities, without defining relevant parameters. TSA told rail operators when the directives were issued that additional performance-based guidance would be provided to clarify the directives requirements, but this information has not been supplied. Further, TSA has not yet developed criteria or procedures for rail inspectors to use in enforcing compliance with the directives. In addition, stakeholders we contacted questioned the extent to which the security directives reflected industry best practices. For example, one requirement of the directives was that the doors of the rail engineer's compartment be locked, which conflicts with an existing FRA safety regulation calling for these doors to remain unlocked for escape purposes. In September 2004, in response to our prior recommendation, DHS and DOT signed a memorandum of understanding (MOU) intended to identify ways to improve coordination and collaboration between and among federal and rail industry stakeholders.[4] As of July 2005, the departments were developing agreements within the framework of this memorandum to delineate specific security-related roles, responsibilities, and resources for mass transit, rail, research and development, and other matters.[5] However, none of the agreements have been finalized and timelines have not been established for doing so. Completing these agreements could help to ensure that federal activities to secure passenger rail systems are coordinated and that stakeholders are appropriately involved in the development and implementation of these activities.

Domestic and foreign passenger rail operators we contacted or visited have generally taken similar actions to help secure their systems against the risk posed by terrorism. Specifically, most U.S. and foreign operators we contacted had implemented customer awareness programs to encourage passengers to remain vigilant and report suspicious activities, increased the number and visibility of their security personnel, increased the usage of canine teams to detect drugs and explosives, enhanced employee training programs, upgraded security technology, tightened access controls, and made system design improvements to enhance security. However, we observed security practices among certain foreign passenger rail systems or their governments that were not in use, at the

[4] GAO, *Mass Transit: Federal Actions Could Help Transit Agencies Address Security Challenges*, GAO-03-263 (Washington, D.C.: Dec. 13, 2002), and *Transportation Security: Federal Action Needed to Help Address Security Challenges*, GAO-03-843 (Washington, D.C.: June 2003).

[5] The Safe, Accountable, Flexible, and Efficient Transportation Equity Act of 2005 (P.L. 109-59) enacted on August 10, 2005, requires DOT and DHS to complete an agreement within 45 days of enactment to define and clarify their respective roles related to public transportation security.

time we completed our fieldwork in June 2005, by the domestic rail operators we contacted or the U.S. government. For example, we found that 2 of 13 foreign rail operators we contacted utilize covert testing to help keep employees alert to security threats. In one type of covert test, suspicious items are placed throughout the rail system and employees are observed to see how long it takes them to find the objects. In addition, 2 of 13 foreign rail operators we visited randomly screen passengers and their baggage. After the July 7, 2005, London bombings, four domestic passenger rail operators began randomly screening passengers and their baggage on a limited basis. Further, in five countries we visited, national governments have centralized research on security technologies and maintain clearinghouses on these technologies and security best practices, giving rail operators a single source for identifying and comparing, among other things, chemical sensors, closed-circuit television, and intrusion detection systems. Introducing any of these security practices into the U.S. rail system may pose political, legal, fiscal, and cultural challenges, but may nevertheless warrant examination to determine whether they could enhance the security of domestic rail systems.

To help ensure that the federal government has the information it needs to prioritize passenger rail assets based on risk, and in order to evaluate, select, and implement commensurate measures to help the nation's passenger rail operators protect their systems against acts of terrorism, we are making several recommendations. Among them, we recommend that TSA establish a plan with timelines for completing its methodology for conducting risk assessments, develop security standards that reflect industry best practices and can be measured and enforced, and set timelines for completing memorandum of understanding agreements. In addition, we are recommending that the Secretary of DHS determine the feasibility, in a risk management context, of implementing certain security practices used by foreign rail operators. These recommendations should be implemented in collaboration with DOT and the passenger rail industry. We provided DHS, DOT, and Amtrak a draft of this report for review and comment. DOT and Amtrak generally agreed with our findings and recommendations and provided technical comments, which we have incorporated where appropriate. DHS generally concurred with the report's recommendations. However, DHS raised questions about, among other things, the extent to which the report reflected the agency's efforts to involve federal and rail industry stakeholders in the development of security directives and criticality assessments. According to TSA, the emergency circumstances under which the directives were issued allowed for only limited input and review by federal and rail industry stakeholders. However, we believe that using the federal rule-making process as a means of establishing permanent standards would make the process more transparent and could help TSA in developing standards that are most appropriate for the industry and which can be measured, monitored, and enforced. These stakeholders will be involved in administering, implementing, and/or enforcing TSA standards and stakeholder buy-in would be critical to the success of such initiatives. DHS's comments appear in appendix IV.

Background

Overview of the U.S. Passenger Rail System

Each weekday, 11.3 million passengers in 35 metropolitan areas and 22 states use some form of rail transit.[6] Heavy rail systems—subway systems like New York City's transit system and Washington, D.C.'s Metro—typically operate on fixed rail lines within a metropolitan area and have the capacity for a heavy volume of traffic. Commuter rail systems typically operate on railroad tracks and provide regional service (e.g., between a central city and adjacent suburbs). Commuter rail systems are traditionally associated with older industrial cities, such as Boston, New York, Philadelphia, and Chicago. Light rail systems are typically characterized by lightweight passenger rail cars that operate on track that is not separated from vehicular traffic for much of the way. All types of rail transit systems in the United States are typically owned and operated by public sector entities, such as state and regional transportation authorities.

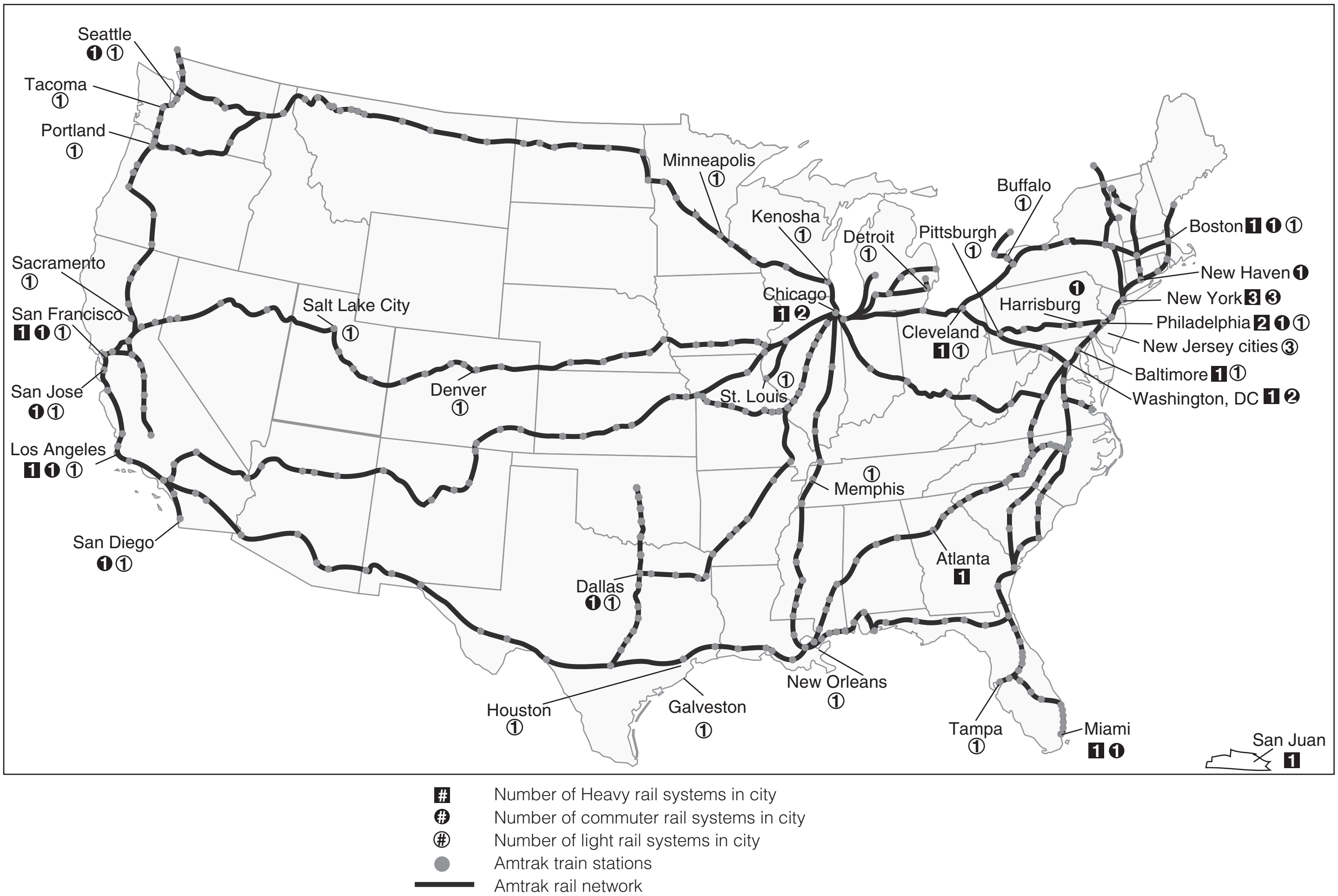
Amtrak operates the nation's primary intercity passenger rail service over a 22,000-mile network, primarily over leased freight railroad tracks.[7] Amtrak serves more than 500 stations (240 of which are staffed) in 46 states and the District of Columbia, and it carried more than 25 million passengers in 2004. According to Amtrak, about two-thirds of its ridership is wholly or partially on the "Northeast Corridor," between Boston and Washington, D.C. Amtrak owns about 650 miles of track, primarily on the Northeast Corridor. Stations are owned by Amtrak, freight carriers, municipalities, and some private entities. Amtrak also operates commuter rail services in certain jurisdictions on behalf of state and regional

[6] The American Public Transportation Association compiled this fiscal year 2003 ridership data from FTA's National Transit Database. These are the most current data available. Rail transit systems in the District of Columbia and Puerto Rico are included in these statistics.

[7] The Alaska Railroad Corporation also operates intercity passenger rail service.

transportation authorities. Figure 1 identifies the geographic location of rail transit systems and Amtrak within the United States.

Figure 1: Geographic Distribution of Amtrak and Rail Transit Systems



Source: Amtrak and National Transit Database.

Passenger Rail Systems Are Inherently Vulnerable to Terrorist Attacks

To date, U.S. passenger rail systems have not been targets of terrorist attacks. However, worldwide, public transportation in general and passenger rail in particular, have been attacked multiple times, sometimes with grave results. According to a database of worldwide terrorist incidents maintained by the RAND Corporation, from 1995 to June 2005, there have been over 250 terrorist attacks worldwide against rail targets, resulting in almost 900 deaths and over 6,000 injuries.[8] Among them were the fatal 1995 sarin gas attack on the Tokyo subway system by the Aum Shinri Kyo doomsday cult, resulting in 12 deaths and 5,000 injuries; the December 2003 bomb attack by Chechen rebels on a Russian commuter train, resulting in 46 fatalities and 165 injuries; and the March 2004 terrorist bombing attacks on commuter trains in Madrid, for which an al Qaeda affiliate organization claimed responsibility, and in which 191 people were killed and 600 were injured.

According to passenger rail officials and passenger rail experts, certain characteristics of domestic and foreign passenger rail systems make them inherently vulnerable to terrorist attacks and therefore difficult to secure. By design, passenger rail systems are open (i.e., have multiple access points, hubs serving multiple carriers, and, in some cases, no barriers) so that they can move large numbers of people quickly. In contrast, the U.S. commercial aviation system is housed in closed and controlled locations with few entry points. The openness of passenger rail systems can leave them vulnerable because operator personnel cannot completely monitor or control who enters or leaves the systems. In addition, other characteristics of some passenger rail systems—high ridership, expensive infrastructure, economic importance, and location (e.g., large metropolitan areas or tourist destinations)—also make them attractive targets for terrorists because of the potential for mass casualties and economic damage and disruption. Moreover, some of these same characteristics make passenger rail systems difficult to secure. For example, the numbers of riders that pass through a subway system—especially during peak hours—may make the sustained use of some security measures, such as metal detectors, difficult because they could result in long lines that could disrupt scheduled service. In addition, multiple access points along extended routes could make the cost of securing each location prohibitive. Balancing the potential economic

[8] These statistics do not include the July 2005 London attacks, which resulted in over 50 fatalities and over 700 injuries.

impacts of security enhancements with the benefits of such measures is a difficult challenge.

Multiple Stakeholders Share Responsibility for Securing Passenger Rail Systems

Securing the nation's passenger rail systems is a shared responsibility requiring coordinated action on the part of federal, state, and local governments; the private sector; and rail passengers who ride these systems. Since the September 11 attacks, the role of federal government agencies in securing the nation's transportation systems, including passenger rail, have continued to evolve. Prior to September 11, DOT—namely FTA and FRA—was the primary federal entity involved in passenger rail security matters. In response to the attacks of September 11, Congress passed the Aviation and Transportation Security Act (ATSA), which created TSA within DOT and defined its primary responsibility as ensuring security in all modes of transportation.[9] The act also gave TSA regulatory authority for security over all transportation modes. ATSA does not specify TSA's roles and responsibilities in securing the maritime and land transportation modes at the level of detail it does for aviation security. Instead, the act broadly identifies that TSA is responsible for ensuring the security of all modes of transportation. With the passage of the Homeland Security Act of 2002, TSA was transferred, along with over 20 other agencies, to the Department of Homeland Security.[10]

With the creation of DHS in 2002, one of its components, ODP, became the primary federal source for security funding for passenger rail systems.[11] ODP is the principal component of DHS responsible for preparing the United States for acts of terrorism and has primary responsibility within the executive branch for assisting and supporting DHS, in coordination with other directorates and entities outside of the department, in

[9] Pub. L. No. 107-71, 115 Stat. 597 (2001).

[10] Pub. L. No. 107-296, 116 Stat. 2135 (2002).

[11] The Department of Justice established ODP in 1998 within the Office of Justice Programs. ODP was subsequently transferred to DHS's Directorate of Border and Transportation Security upon DHS's creation in March 2003 (Homeland Security Act of 2002, section 403(5), 6 U.S.C. 203(5)). In March 2004, the Secretary of Homeland Security consolidated ODP with the Office of State and Local Government Coordination to form the Office of State and Local Government Coordination and Preparedness (SLGCP). SLGCP, which reports directly to the DHS Secretary, was created to provide a "one-stop shop" for the numerous federal preparedness initiatives applicable to state and local governments. The proposed reorganization of DHS may result in transferring portions of ODP to a newly established Directorate of Preparedness.

conducting risk analysis and risk management activities of state and local governments.[12] In carrying out its mission, ODP provides training, funds for the purchase of equipment, support for the planning and execution of exercises, technical assistance, and other support to assist states, local jurisdictions, and the private sector to prevent, prepare for, and respond to acts of terrorism. Through the Urban Area Security Initiative (UASI) grant program, ODP has provided grants to urban areas to help enhance their overall security and preparedness level to prevent, respond to, and recover from acts of terrorism. In 2003 and 2004, $65 million and $50 million, respectively, were allocated to rail transit agencies through the UASI program. In addition, the DHS Appropriations Act of 2005 appropriated $150 million for rail transit, intercity passenger rail, freight rail, and transit agency security grants. [13] This funding has allowed ODP to build upon the work under way through the UASI program and create and administer two new programs focused specifically on transportation security, the Transit Security Grant Program and the Intercity Passenger Rail Security Grant Program. These programs provide financial assistance to address security preparedness and enhancements for transit (to include commuter, heavy, and light rail systems, intracity bus, and ferry), and intercity rail (Amtrak) systems. The grant programs specifically provide funding for the prevention and detection of explosive devices and chemical, biological, radiological, and nuclear agents. About $108 million was provided to rail transit agencies and $7.1 million to Amtrak through these grant programs in 2005.[14]

While TSA is the lead federal agency for ensuring the security of all transportation modes, FTA conducts nonregulatory safety and security activities, including safety- and security-related training, research, technical assistance, and demonstration projects. In addition, FTA promotes safety and security through its grant-making authority. FTA provides financial assistance to rail transit agencies to plan and develop new systems and operate, maintain, and improve existing systems. FTA stipulates conditions of grants, such as certain safety and security statutory and regulatory requirements, and FTA may withhold funds for

[12] At the time of our review, DHS was undertaking a departmentwide reorganization that will affect both the structure and functions of DHS directorates and component agencies.

[13] Pub. L. No. 108-334, 118 Stat. 1298 (2004).

[14] The remaining funds were used to provide security grants for intracity bus and freight rail systems and for technical assistance and management and administration purposes. 49 USC 5307 (d)(1)(J)(i).

noncompliance with the conditions of a grant.[15] While FTA cannot regulate safety and security operations at transit agencies,[16] FRA has regulatory authority for rail safety over commuter rail operators and Amtrak, and employs over 400 rail inspectors that periodically monitor the implementation of safety and security plans at these systems.[17]

State and local governments, passenger rail operators, and private industry are also important stakeholders in the nation's rail security efforts. State and local governments play a vital role, in part, because they may own or operate a significant portion of the passenger rail system. Even when state and local governments are not owners and operators, they are directly affected by passenger rail systems that run within and through their jurisdictions. Consequently, the responsibility for responding to emergencies involving the passenger rail infrastructure often falls to state and local governments.

Passenger rail operators, which can be public or private entities, are responsible for administering and managing passenger rail activities and services, including security. Passenger rail operators can directly operate the service provided or contract for all or part of the total service. Although all levels of government are involved in passenger rail security, the primary responsibility for securing passenger rail systems rests with the passenger rail operators. We discuss actions taken by federal agencies and passenger rail operators to enhance security in more detail later in this report.

[15] For example, transit agencies must spend 1 percent of their urbanized area formula funds on security improvements. FTA is to verify that agencies comply with this requirement and may withhold funding from agencies that it finds are not in compliance. Agencies are not required to comply with this spending rule if a valid justification can be documented, such as state and local funds for security are inadequate or security trend data do not warrant security spending.

[16] 49 U.S.C. 5324(c). FTA has regulatory authority for state safety oversight of rail fixed-guideway systems and a drug and alcohol program. DOT is responsible for regulating the safety of transit agencies.

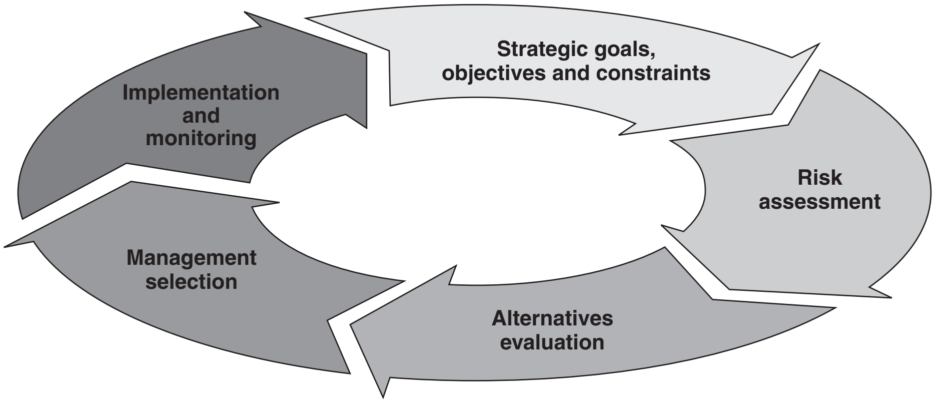
[17] FRA administers and enforces the federal laws and related regulations that are designed to promote safety on railroads, such as track maintenance, inspection standards, equipment standards, and operating practices. FRA exercises jurisdiction over all areas of railroad safety under 49 U.S.C. 20103.

Assessing and Managing Risks to Rail Infrastructure Using a Risk Management Approach

In recent years, we, along with Congress (most recently through the Intelligence Reform and Terrorism Prevention Act of 2004),[18] the executive branch (e.g., in presidential directives), and the 9/11 Commission have required or advocated that federal agencies with homeland security responsibilities utilize a risk management approach to help ensure that finite national resources are dedicated to assets or activities considered to have the highest security priority. We have concluded that without a risk management approach, there is limited assurance that programs designed to combat terrorism are properly prioritized and focused. Thus, risk management, as applied in the homeland security context, can help to more effectively and efficiently prepare defenses against acts of terrorism and other threats.

A risk management approach entails a continuous process of managing risk through a series of actions, including setting strategic goals and objectives, performing risk assessments, evaluating alternative actions to reduce identified risks by preventing or mitigating their impact, selecting actions to undertake by management, and implementing and monitoring those actions. Figure 2 depicts a risk management cycle that is our synthesis of government requirements and prevailing best practices previously reported.

Figure 2: Risk Management Cycle


Strategic goals, objectives and constraints
Risk assessment
Alternatives evaluation
Management selection
Implementation and monitoring

Source: GAO.

[18] Pub. L. No. 108-458, 118 Stat. 3638.

Setting strategic goals, objectives, and constraints is a key first step in implementing a risk management approach and helps to ensure that management decisions are focused on achieving a strategic purpose. These decisions should take place in the context of an agency's strategic plan that includes goals and objectives that are clear, concise, and measurable.

Risk assessment, a critical element of a risk management approach, helps decision makers identify and evaluate potential risks so that countermeasures can be designed and implemented to prevent or mitigate the effects of the risks. Risk assessment is a qualitative and/or quantitative determination of the likelihood of an adverse event occurring and the severity, or impact, of its consequences. Risk assessment in a homeland security application often involves assessing three key elements—threat, criticality, and vulnerability:

- A threat assessment identifies and evaluates potential threats on the basis of factors such as capabilities, intentions, and past activities.
- A criticality or consequence assessment evaluates and prioritizes assets and functions in terms of specific criteria, such as their importance to public safety and the economy, as a basis for identifying which structures or processes are relatively more important to protect from attack.
- A vulnerability assessment identifies weaknesses that may be exploited by identified threats and suggests options to address those weaknesses.

Information from these three assessments contributes to an overall risk assessment that characterizes risks on a scale such as high, medium, or low and provides input for evaluating alternatives and management prioritization of security initiatives.[19] Additional details on these assessment elements can be found in appendix II. The risk assessment element in the overall risk management cycle may be the largest change from standard management steps and is central to informing the remaining steps of the cycle.

[19] GAO, *Transportation Security: Systematic Planning Needed to Optimize Resources*, GAO-05-357T (Washington D.C.: Feb. 15, 2005); *Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts*, GAO-02-208T (Washington, D.C.: Oct. 31, 2001); *and Combating Terrorism: Threat and Risk Assessments Can Help Prioritize and Target Program Investments*, GAO/NSIAD-98-74 (Washington, D.C.: April 9, 1998).

The next step in a risk management approach—alternatives evaluation—considers what actions may be needed to address identified risks, the associated costs of taking these actions, and any resulting benefits. This information is then to be provided to agency management to assist in the selection of alternative actions best suited to the unique needs of the organization. An additional step in the risk management approach is the implementation and monitoring of actions taken to address the risks, including evaluating the extent to which risk was mitigated by these actions. Once the agency has implemented the actions to address risks, it should develop criteria for and continually monitor the performance of these actions to ensure that they are effective and also reflect evolving risk.

Federal Agencies with Risk Management Responsibilities

A number of federal departments and agencies have risk management and critical infrastructure protection responsibilities stemming from various requirements. The Homeland Security Act of 2002, which created DHS, directed the department's Information Analysis and Infrastructure Protection (IAIP) Directorate to utilize a risk management approach in coordinating the nation's critical infrastructure protection efforts. This includes using risk assessments to set priorities for protective and support measures by the department, other federal agencies, state and local government agencies and authorities, the private sector, and other entities. Homeland Security Presidential Directive 7 (HSPD-7) defines critical infrastructure protection responsibilities for DHS, sector-specific agencies (those federal agencies given responsibility for transportation, energy, telecommunications, and so forth), and other departments and agencies. The President instructs federal departments and agencies to identify, prioritize, and coordinate the protection of critical infrastructure to prevent, deter, and mitigate the effects of terrorist attacks. The Secretary of DHS is assigned several responsibilities by HSPD-7, including establishing uniform polices, approaches, guidelines, and methodologies for integrating federal infrastructure protection and risk management activities within and across sectors. To ensure the coverage of critical sectors, HSPD-7 designated sector-specific agencies for 17 critical infrastructure sectors.[20] These agencies are responsible for infrastructure

[20] Sector-specific agencies have been designated for the following sectors: transportation; agriculture and food; public health and health care; drinking water and wastewater treatment; energy; banking and finance; national monuments and icons; defense industrial base; information technology; telecommunications; chemical; emergency services; postal and package shipping; dams; government facilities; commercial facilities; and nuclear reactors, materials, and waste.

protection activities in their assigned sectors, including coordinating and collaborating with relevant federal agencies, state and local governments, and the private sector to carry out their responsibilities and facilitating the sharing of information about vulnerabilities, incidents, potential protective measures, and best practices.

Pursuant to HSPD-7 and the National Infrastructure Protection Plan (NIPP), DHS was designated as the sector-specific agency for the transportation sector, a responsibility the department has delegated to TSA.[21] As the sector-specific agency for transportation, TSA is required to develop a transportation sector-specific plan (TSSP) for identifying, prioritizing, and protecting critical transportation infrastructure and key resources that will provide key input to the broader NIPP to be prepared by IAIP. DHS issued an interim NIPP in February 2005 that was intended to serve as a road map for how DHS and stakeholders—including other federal agencies, the private sector, and state and local governments—should use risk management principles for determining how to prioritize activities related to protecting critical infrastructure and key resources within and among each of the 17 sectors in an integrated, coordinated fashion. DHS expects the next iteration of the NIPP to be issued in November 2005, with the sector-specific plans, including the TSSP, being incorporated into this plan in February 2006. HSPD-7 also requires DHS to coordinate with DOT on all transportation security matters. Table 1 summarizes selected responsibilities for federal agencies with lead or supporting roles for critical infrastructure protection and risk management efforts.

[21] The transportation sector includes mass transit; aviation; maritime; ground/surface; and rail and pipeline systems.

Table 1: Selected Roles and Responsibilities of Federal Agencies Related to Risk Management and Critical Infrastructure Protection

Statute or directive	Agency with lead or supporting role	Selected responsibilities	Related output of action	Due date
Homeland Security Act of 2002	IAIP[a]	**Coordinates national critical infrastructure protection (CIP) efforts by**: • conducting risk assessments of key resources and critical infrastructure to determine the risks posed by terrorist attacks within the United States; • integrating relevant information, analyses, and assessments (whether conducted by department or others) in order to identify priorities for protective and support measures; • recommending measures to protect the key resources and critical infrastructure of the United States in coordination with other federal agencies and in cooperation with state and local government agencies and authorities, the private sector, and other entities.	Develop a comprehensive national plan for securing the key resources and critical infrastructure	Not specified
	ODP[a]	**As the principal federal agency in preparing the United States for acts of terrorism**: • assists and supports DHS in conducting appropriate risk analysis and risk management activities of state, local, and tribal governments; • serves as primary office responsible for providing training, funds for the purchase of equipment, support for the planning and execution of exercises.	Risk analysis and risk management activities for states and local jurisdictions	Not applicable
Homeland Security Presidential Directive-7	IAIP[b]	**Coordinate national CIP efforts by:** • identifying, prioritizing, and coordinating the protection of critical infrastructure, emphasizing protection against catastrophic health effects or mass casualties; • establishing uniform policies, approaches, guidelines, and methodologies for integrating federal infrastructure protection and risk management activities within and across sectors.	National Infrastructure Protection Plan	12/04

Statute or directive	Agency with lead or supporting role	Selected responsibilities	Related output of action	Due date
	TSA[c]	**As sector-specific agency for transportation:** • identify, prioritize, and coordinate the protection of critical transportation systems infrastructure, including conducting and facilitating vulnerability assessments and encouraging risk management strategies; • coordinate and collaborate with relevant federal agencies, state and local governments, and the private sector.	Transportation Sector-Specific Plan	12/04
	DOT[d]	**Support CIP activities in transportation sector by:** • collaborating with DHS on all matters relating to transportation security and transportation infrastructure protection.	Not applicable	Not applicable
Intelligence Reform and Terrorism Prevention Act of 2004	TSA[e]	**Develop, prepare, implement, and update as needed a National Strategy for Transportation Security, including:** • development of transportation modal security plans; • identification and evaluation of transportation assets that must be protected from terrorist attack; • development of risk-based priorities across all transportation modes and realistic deadlines for addressing security needs associated with those assets.	National Strategy for Transportation Security	4/05
	DOT	**Works jointly with DHS to develop, revise, and update the National Strategy for Transportation Security**	Not applicable	Not applicable

Source: GAO analysis of federal roles and responsibilities related to risk management and critical infrastructure protection.

[a] Lead role designated by statute.

[b] Lead role for all sectors; responsibility delegated by DHS.

[c] Lead role for transportation sector; responsibility delegated by DHS.

[d] Supporting role for DHS.

[e] Lead role delegated by DHS.

DHS Has Taken Steps to Assess Risk to Passenger Rail Systems, but Additional Work Is Needed to Guide Security Investments

DHS component agencies have taken various steps to assess the risk posed by terrorism to U.S. passenger rail systems. ODP has developed and implemented a risk assessment methodology intended to help passenger rail operators and others enhance their capacity to respond to terrorist incidents and identify and prioritize security countermeasures. As of July 2005, ODP had completed 7 risk assessments with rail operators and 12 others were under way. Further, TSA completed a threat assessment for mass transit and rail and has begun to identify critical rail assets, but it has not yet completed an overall risk assessment for the passenger rail industry. DHS is developing guidance to help these and other sector-specific agencies work with stakeholders to identify and analyze risk.

ODP Has Worked with Passenger Rail Operators to Develop Risk Assessments to Help Prioritize Rail Security Needs and Investments

In 2002, ODP began conducting risk assessments of passenger rail operators through its Mass Transit Technical Assistance program. These assessments are intended to help passenger rail operators and port authorities enhance their capacity and preparedness to respond to terrorist incidents involving weapons of mass destruction, and identify and prioritize security countermeasures and emergency response capabilities. ODP's approach to risk assessment is generally consistent with the risk assessment component of our risk management approach. The agency has worked with passenger rail operators and others to complete several risk assessments. As of July 2005, ODP had completed 7 risk assessments in collaboration with passenger rail operators.[22] Twelve additional risk assessments are under way, and an additional 11 transit agencies have requested assistance through this program.

ODP's methodology for conducting risk assessments is articulated in a tool kit designed to enable passenger rail operators and others to compare relative risks among assets, identify assets with a perceived high level of risk, and prioritize measures to mitigate those risks.[23] Once ODP and a rail operator agree to collaborate on the risk assessment, ODP sends a

[22] ODP has completed risk assessments with the Port Authority of New York and New Jersey, New Jersey Transit, Massachusetts Bay Transportation Authority, Washington Metropolitan Area Transit Authority, Southeastern Pennsylvania Transportation Authority, Tri-County Metropolitan Transportation District of Oregon, and the Delaware River Port Authority.

[23] According to ODP, risk assessment methodologies from a variety of sources were reviewed as part of the tool kit's development, including various state transportation risk assessment methods, airport vulnerability methods, and DOT infrastructure assessment methods.

technical assistance team consisting of experts in the risk management and emergency response field to visit the rail operator on-site to support the implementation of the risk assessment process. The team assists the operator in using the tool kit to generate information on criticality, threat, vulnerability, impact, and risk. Once completed, the documented results should serve as a guide for future applications of the risk assessment process to keep pace with new threat information and newly vulnerable assets.

ODP's risk assessment process involves, first, an analysis of four elements—criticality, threat, vulnerability, and impact. Using the tool kit, the operator begins by conducting the criticality assessment to identify and prioritize *critical assets* based upon factors such as the potential for serious injury or loss of life, or the economic implications on the livelihood, resources, or wealth of the area, region, or country if the asset was destroyed. Assets deemed to be "most critical" are then evaluated using the remaining risk assessment components. The operator then conducts the *threat assessment* to identify the range of weapon types that terrorists might use against the operator's critical assets, establish the likelihood that critical assets might be targeted, and develop possible attack scenarios. These attack scenarios are then used to perform a vulnerability assessment that evaluates the susceptibility of critical assets to these scenarios and determines such things as the probability of an attack succeeding and whether it can be stopped. Once these first three assessment components are completed, the operator determines the impact that the partial or complete destruction of a critical asset would have on the asset's ability to function based upon specific threat scenarios. Table 2 describes selected steps that operators take, in conjunction with ODP, to carry out these four assessment components using ODP's risk assessment tool kit.

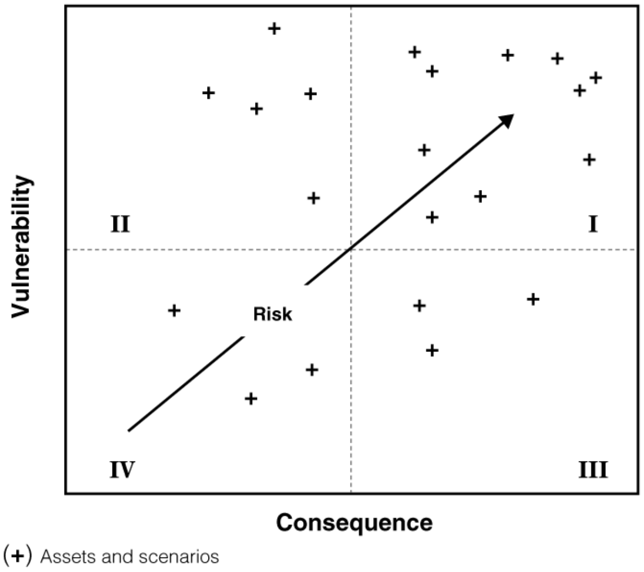
Table 2: Selected Steps in ODP's Risk Assessment Process

Assessment component	Assessment steps
Criticality	Step 1. Develop a worksheet of candidate critical assets (i.e., infrastructure, facilities, equipment, and personnel) that enable the operator to achieve its mission. Step 2. Establish critical asset factors—factors that describe the characteristics of assets that would result in significant negative impact to the operator given their loss in a terrorist event (i.e., economic impact, symbolic importance, functional importance). Step 3. Assign quantitative values to each factor that indicate the importance of the factor to the overall mission of the operator. Step 4. Apply the factors to the list of candidate assets to develop a criticality score. Step 5. Prioritize assets based upon their criticality scores. Rail operator officials review rankings to determine their reasonableness and to establish a threshold for the assets considered most critical.
Threat	Step 1. Develop a list of weapons types (i.e., large or small explosives, biological conventional explosive, nuclear device) that might be used by terrorists. Step 2. Evaluate the selected weapon types on the likelihood (using a five-point scale) that terrorists have each weapon and would use it against the operator's assets. Step 3. Evaluate the attractiveness of targets based on the potential for casualties, potential for economic disruption, and symbolic importance. Step 4. Define attack scenarios (based on target asset, weapon, and mode of delivery); the information will be used in subsequent assessment components.
Vulnerability	Step 1. Develop a rating to determine the probability of a successful attack. Rating is based upon three factors: the ability to limit or deny ingress and egress to an asset by a terrorist (access control), the ability to expose or reveal an attack before it takes place (detection capabilities), the ability to interdict once an attack has been detected (interdiction capabilities). Step 2. Using these probability ratings, develop an overall vulnerability rating that represents the relative likelihood of an attack being attempted and successfully carried out.
Impact	Step 1. Use the critical asset factors identified above to rate the effect of a weapon on each asset's mission. Step 2. Once each asset has been rated, use a mathematical formula to calculate a total overall impact level—how each asset's mission is affected based upon the extent to which it would be destroyed.

Source: GAO analysis of ODP information.

The results developed in the threat, criticality, vulnerability, and impact assessments are then used to develop an overall risk assessment in order to evaluate the relative risk among various assets, weapons, and modes of attack. This is intended to give operators an indication of which asset types and threat scenarios carry the highest risk and that, accordingly, are likely candidates for early risk mitigation action. Using the results of the risk assessment process, a diagram of relative risk is developed by plotting the assets and scenarios in terms of vulnerability and consequence, as shown in figure 3.[24]

Figure 3: Sample ODP Relative Risk Diagram



Source: ODP.

By showing the relative risk of all assets and scenarios identified, this diagram identifies the assets and scenarios that have the greatest estimated level of relative risk and provides critical information useful to develop and prioritize security countermeasures. According to ODP, assets with scenarios that fall in quadrants I and III have the greatest potential negative impact (i.e., the greatest consequence) on an operator's system if attacked. Assets with scenarios that fall in quadrants I and II have the greatest vulnerability to attack. Therefore, quadrant I contains the assets and scenarios that have the greatest vulnerability and negative consequence and are likely candidates for early mitigation action from a policy decision-making perspective.

According to rail operators who have used ODP's risk assessment methodology and commented about it to DHS or us, the method has been successful in helping to devise risk reduction strategies to guide security-

[24] "Consequence" is defined as the portion of an asset's criticality that would be reduced as a result of a successful attack.

related investments. For example, between September 2002 and March 2003, ODP's technical assistance team worked with the Port Authority of New York and New Jersey (PANYNJ) to conduct a risk assessment of all of its assets—its Port Authority Trans-Hudson (PATH) passenger rail system, as well as airports, ports, interstate highway crossings, and commercial properties.[25] According to PANYNJ officials, the authority was able to develop and implement a risk reduction strategy that enabled it to identify and set priorities for improvements in security and emergency response capability that are being used to guide security investments.

As part of this risk assessment, PANYNJ identified and prioritized particular types of security countermeasures that, if implemented, would improve the authority's overall risk profile by moving assets into the lower parts of the risk diagram (as shown in fig. 3). Examples of countermeasures considered include site-hardening of assets such as bridges and tunnels; increased patrols, guards, and canine units; event-activated closed-circuit television (CCTV); and intrusion detection systems. According to PANYNJ officials, the associated costs and benefits of the countermeasures identified were considered, and management was involved in choosing and prioritizing the actions included in the plan. More specifically, according to authority officials, the risk assessment was instrumental in obtaining management approval for a 5-year, $500 million security capital investment program, as it provided a risk-based justification for these investments.[26] Examples of passenger rail security capital investments PANYNJ is making as part of this program include the development of a state-of-the art system wide security operations center for the PATH system, access control and alarm monitoring system replacement at 45 locations, and digital video recording upgrades to its

[25] PANYNJ is a bistate public agency that manages and maintains bridges, tunnels, bus terminals, airports, the PATH passenger rail system, and seaports in the greater New York/New Jersey metropolitan area. PANYNJ was also the property owner and operator of the World Trade Center site and the PATH passenger rail station underneath the site that was destroyed by the September 11 terrorist attacks. At the request of PANYNJ, ODP's technical assistance team worked with authority personnel to conduct the first risk assessment using ODP's model. This collaborative effort provided the means for ODP to test and refine its methodology and develop the tool kit now in use.

[26] On the basis of the ODP and prior risk assessments and identified risks, PANYNJ identified approximately $1 billion dollars in security investments or actions. The current $500 million capital investment program was based directly on the highest risks identified in the assessment. The initial $500 million program did not include countermeasures identified by the assessments that could not be implemented immediately. For example, the authority viewed countermeasures, such as weapons of mass destruction detection systems, as cost-prohibitive until technological advances are made in this arena.

CCTV system. At the time of our review, the authority was 2 years into implementing the strategy and associated capital investment program and had just completed its first risk assessment update. PANYNJ officials told us they have formally incorporated the ODP risk assessment model into the authority's annual planning and budgeting cycle and are able to track and assess how security projects improve the authority's overall risk profile. PANYNJ staff are now working on a cost-benefit module to be included in the authority's risk assessment program, with the objective of making more discrete trade-offs among high-cost security programs on the basis of which ones provided the highest payoff.

The six other passenger rail operators that have completed ODP's risk assessment process also stated that they valued the process. Specifically, operators said that the assessments enabled them to prioritize investments based on risk and are already allowing or are expected to allow them to effectively target and allocate resources toward security measures that will have the greatest impact on reducing risk across their system. For example, one rail operator stated that it is planning on spending its fiscal year 2005 Transit Security Grant Program funding to expand its CCTV coverage, with a focus on stations that serve major public gatherings but do not have such equipment, a measure identified by the risk assessment as the second most effective risk reduction measure to implement. [27] In addition, as a result of the assessment, the operator said that it has incorporated CCTVs into its standard design criteria for new system construction, such as stations and parking garages.

ODP Has Sought to Promote Risk-Based Decision Making among Federal Agencies and Rail Operators

On the basis of its own experience with conducting risk assessments in the field, and in keeping with its mission to develop and implement a national program to enhance the capacity of state and local agencies to respond to incidents of terrorism, ODP has offered to help other DHS components and federal agencies to develop risk assessment tools, according to ODP officials. For example, ODP is partnering with the FRA, TSA, the American Association of Railroads (AAR), and others to develop a risk assessment

[27] The assessment identified the most effective risk reduction measure as training employees and informing the public to serve as the "eyes and ears" and report suspicious objects and behaviors. While, according to the agency, it had undertaken comprehensive steps in these areas, the assessment pointed out the usefulness of making these efforts a permanent part of training, procedures, and public information.

tool for freight rail corridors.[28] In a separate federal outreach effort, ODP worked with TSA to establish a Federal Risk Assessment Working Group to promote interagency collaboration and information sharing. Representatives from participating federal agencies meet monthly to encourage information sharing regarding risk assessments and other related homeland security issues.[29] The working group has, among other things, created a Web-based calendar so participating agencies can upload and share information regarding planned assessments. The calendar also contains detailed information on assessments, including locations, dates, types of assessment, and points of contact.

In addition, in keeping with its mission to deliver technical assistance and training, ODP has partnered with the American Public Transportation Association (APTA) to inform passenger rail operators about its risk assessment technical assistance program.[30] Since June 2004, ODP has attended five APTA conferences or workshops where it has set up information booths, made the tool kit available, and conducted seminars to educate passenger rail operators about the risk assessment process and its benefits. According to an APTA official, ODP's risk assessment technical assistance program has been well received by the transit community. The program is dependent on funding available in ODP's technical assistance budget for support. In fiscal years 2004 and 2005, the program received $5.2 million and $5.7 million, respectively, through ODP's technical assistance budget.

ODP has leveraged its grant-making authority to promote risk-based funding decisions for passenger rail. For example, passenger rail operators must have completed a risk assessment to be eligible for financial

[28] The American Association of Railroads is an association representing the interests of the rail industry, focused mostly at the federal level. Its members are primarily freight rail operators in the United States, Canada, and Mexico. However, it also represents some passenger rail interests, including Amtrak.

[29] Participating agencies include DHS's Office of State and Local Government Coordination and Preparedness, DHS's U.S. Coast Guard, DHS's Information Analysis and Infrastructure Protection Directorate, the Department of Defense's U.S. Transportation Command, DOT's Federal Transit Administration, and DOT's Federal Highway Administration.

[30] The American Public Transportation Association is a nonprofit trade association representing over 1,500 public and private member organizations, including transit systems and commuter rail operators; planning, design, construction, and finance firms; product and service providers; academic institutions; transit associations; and state departments of transportation.

assistance through the fiscal year 2005 Transit Security Grant program administered by ODP. To receive these funds, passenger rail operators are also required to have a security and emergency preparedness plan that identifies how the operator intends to respond to security gaps identified by risk assessments. This plan, along with a regional transit security strategy prepared by regional transit stakeholders, will serve as the basis for determining how the grant funds are to be allocated.

Risk assessments are also a key driver of federal funds distributed through ODP's fiscal year 2005 Intercity Passenger Rail Grant Program. This $7.1 million program provides financial assistance to Amtrak for the protection of critical infrastructure and emergency preparedness activities along Amtrak's Northeast Corridor and its hub in Chicago. Amtrak is required to conduct a risk assessment of these areas in collaboration with ODP, in order to receive the grant funds.[31] A recent review of Amtrak's security posture and programs conducted by the RAND Corporation and funded by FRA in 2004 found that no comprehensive terrorism risk assessment of Amtrak has been conducted that would provide an empirical baseline for investment prioritization and decision making for Amtrak's security policies and investment plans. As another condition for receiving the grant funds, Amtrak is required to develop a security and emergency preparedness plan that, along with the risk assessment, is to serve as the basis for proposed allocations of grant funding. According to an Amtrak security official, it welcomes the risk assessment effort and plans to use the results of the assessment to guide its security plans and investments. According to ODP officials, as of July 2005, the Amtrak risk assessment was nearly 50 percent complete.

TSA Has Begun to Assess Risks to Passenger Rail

As the agency responsible for ensuring the security of all modes of transportation, TSA has been charged by DHS with fulfilling key requirements of HSPD-7 and the Intelligence Reform and Terrorism Prevention Act of 2004. Specifically, TSA is required to conduct and

[31] Up to 30 percent of the available funds will be available to assist Amtrak in meeting its most pressing security needs in the Northeast Corridor and Chicago (as identified through previously conducted site-specific assessments) prior to completion of the risk assessment. However, the remainder of the grant funds will not be released until Amtrak has completed the risk assessment and also submitted a security and emergency preparedness plan. Amtrak is also required to demonstrate that its planning process and allocations of funds are fully coordinated with regional planning efforts in the National Capitol Region, Philadelphia, New York, Boston, and Chicago. Amtrak is using approximately $700,000 of the grant funds for the ODP risk assessment.

facilitate risk assessments in order to identify, prioritize, and coordinate the protection of critical transportation systems infrastructure, as well as develop risk-based priorities across all transportation modes. As part of this effort, TSA is required to develop plans that, among other things, identify and prioritize critical transportation assets for protection. At the time of our review, TSA had taken steps to meet these responsibilities but had not yet completed the risk assessments for the rail industry (among others) or the plans that they support as required.

In October 2004, TSA completed an overall threat assessment for both mass transit and passenger and freight rail modes.[32] TSA began conducting a second risk assessment element—criticality assessments of passenger rail stations—in the spring of 2004, but the effort had not been completed at the time of our review. According to TSA, a criticality assessment tool was developed that considers multiple factors, such as the potential for loss of life or effects on public health; the economic impact of the loss of function of the asset and the cost of reconstitution; and the local, regional, or national symbolic importance of the asset. These factors were to be used to arrive at a criticality score that, in turn, would enable the agency to rank assets and facilities based on relative importance, according to TSA officials.

To date, TSA has assigned criticality scores to nearly 700 passenger rail stations. In May 2005, TSA began conducting assessments for other passenger rail assets such as bridges and tunnels. TSA officials told us that as of July 2005, they had completed 73 criticality assessments for bridge and tunnel assets and expect to conduct approximately 370 additional assessments in these categories. Once TSA has completed its criticality assessment, a senior group of transportation security experts will review these scores and subsequently rank and prioritize them. As of July 2005, TSA had not established a time frame for completing criticality assessments for passenger rail assets or for ranking assets, and had not identified whether it planned to do so.

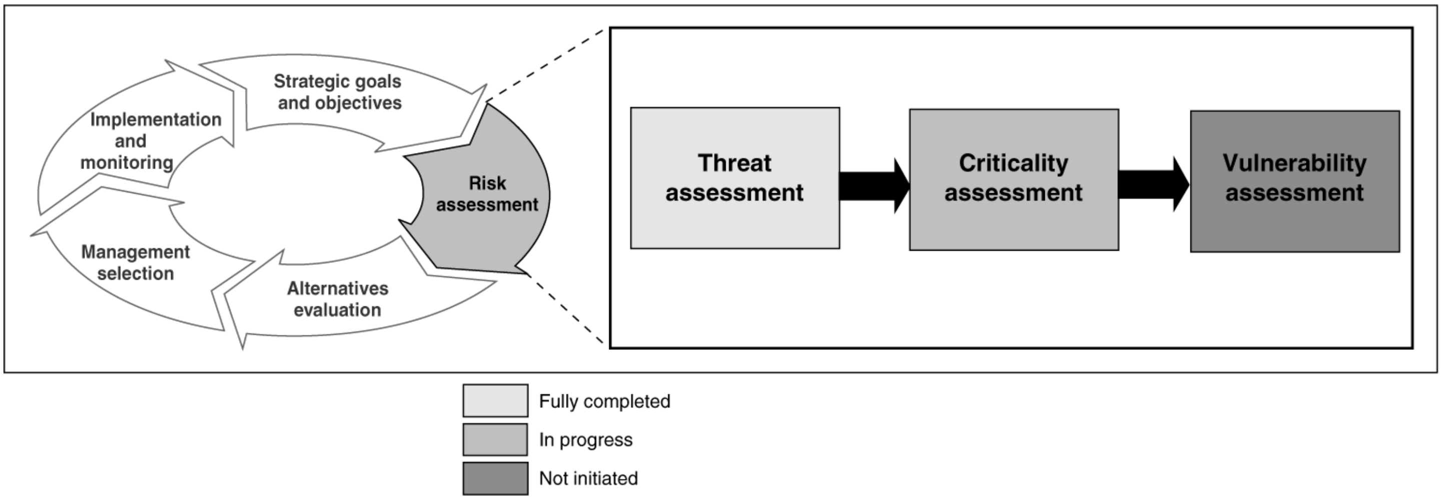
In 2003, TSA officials stated that they planned to work with transportation stakeholders to rank assets and facilities in terms of their criticality. HSPD-7 requires sector-specific agencies such as TSA to collaborate with all relevant stakeholders, including federal departments and agencies,

[32] The results of TSA's passenger and freight rail threat assessments contain information that is security sensitive or classified and therefore cannot be disclosed in this report.

state and local governments, and others. In addition, DHS's interim NIPP states that sector-specific agencies, such as TSA, are expected to work with stakeholders—such as rail operators—to determine the most effective means of obtaining and analyzing information on assets. While TSA's methodology for conducting criticality assessments calls for "facilitated sessions" involving TSA modal specialists, DOT modal specialists, and trade association representatives, these sessions with stakeholders have not been held. According to TSA officials, their final methodology for conducting criticality assessments did not include DOT modal specialists and trade associations. With respect to rail operators, TSA officials explained that their risk assessment process does not require operators' involvement. TSA analysts said they have access to a great deal of information (such as open source records, satellite imagery, and insurance industry data) that can facilitate the assessment process. However, when asked to comment on TSA's ability to identify critical assets in passenger rail systems, APTA officials and 10 rail operators we interviewed told us it would be difficult for TSA to complete this task without their direct input and rail system expertise.

TSA plans to rely on asset criticality rankings to prioritize which assets it will focus on in conducting vulnerability assessments. That is, once an asset, such as a passenger rail station, is deemed to be most critical, then TSA would focus on determining the station's vulnerability to attacks. TSA plans to conduct on-site vulnerability assessments for those assets deemed most critical. For assets that are deemed to be less critical, TSA has developed a software tool that it has made available to passenger rail and other transportation operators for them to use on a voluntary basis to assess the vulnerability of their assets. As of July 2005, the tool had not yet been used. According to APTA officials, passenger rail operators may be reluctant to provide vulnerability information to TSA without knowing how the agency intends to use such information. According to TSA, it is difficult, if not impossible, to project any timelines regarding completion of vulnerability assessments in the transportation sector because rail operators are not required to submit them. In this regard, while the rail operators are not required to submit this information, as the sector-specific agency for transportation, TSA is required by HSPD-7 to complete vulnerability assessments for the transportation sector. Figure 4 illustrates the overall progress TSA had made in conducting risk assessments for passenger rail assets as of July 2005.

Figure 4: Status of TSA's Passenger Rail Risk Assessment Efforts, as of July 2005



Source: GAO.

We recognize that TSA's risk assessment effort is still evolving and TSA has had other pressing priorities, such as meeting the legislative requirements related to aviation security. However, until all three assessments of rail systems—threat, criticality, and vulnerability—have been completed in sequence, and until TSA determines how to use the results of these assessments to analyze and characterize risk (e.g., whether high, medium, or low), it may not be possible to prioritize passenger rail assets and guide investment decisions about protecting them.

Finalizing a methodology for assessing risk to passenger rail and other transportation assets and conducting the assessments are key steps needed to produce the plans required by HSPD-7 and the Intelligence Reform and Terrorism Prevention Act of 2004. DHS and TSA have missed both deadlines for producing these plans. Specifically, DHS and TSA have yet to produce the TSSP required by HSPD-7 to be issued in December of 2004, though a draft was prepared in November 2004. DHS and TSA officials told us that they expected the first version of the TSSP to be completed in February 2006. DHS and TSA also missed the April 1, 2005, deadline for completing the national strategy for transportation security required by the Intelligence Reform and Terrorism Prevention Act of 2004. In an April 2005 letter to Congress addressing the missed deadline, the DHS Deputy Secretary identified the need to more aggressively coordinate the development of the strategy with other relevant planning work such as the TSSP, to include further collaboration with DOT modal administrations and DHS components. The Deputy Secretary further stated that DHS expected to finish the strategy within 2 to 3 months. However, as of July 31, 2005, the strategy had not been completed. In April 2005, senior DHS and TSA officials told us that in addition to DOT, industry groups such as APTA and AAR would also be more involved in developing the TSSP and other strategic plans. However, as of July 2005, TSA had not yet engaged these stakeholders in the development of these plans.

DHS Faces Challenges in Comparing and Reconciling Risks and Prioritizing Investments within and across Sectors

As TSA, other sector-specific agencies, and ODP move forward with risk assessment activities, DHS is concurrently developing guidance intended to help these agencies work with their stakeholders to assess risk. HSPD-7 requires DHS to establish uniform policies, approaches, guidelines, and methodologies for integrating federal infrastructure protection and risk management activities within and across sectors. To meet this requirement, DHS has, among other things, been working for nearly 2 years on a risk assessment framework through IAIP.[33] This framework is intended to help the private sector and state and local governments to develop a consistent approach to analyzing risk and vulnerability across infrastructure types and across entire economic sectors, develop consistent terminology, and foster consistent results. The framework is also intended to enable a federal-level assessment of risk in general, and comparisons among risks, for purposes of resource allocation and response planning. DHS has informed TSA that this framework will provide overarching guidance to sector-specific agencies on how various risk assessment methodologies may be used to analyze, normalize, and prioritize risk within and among sectors. The interim NIPP states that the ability to rationalize, or normalize, results of different risk assessments is an important goal for determining risk-related priorities and guiding investments. One core element of the DHS framework—defining concepts, terminology, and metrics for assessing risk—has yet to be completed. The completion date for this element—initially due in September 2004—has been extended twice, with the latest due date in June 2005. However, as of July 31, 2005, this element has not been completed.

Because neither this element nor the framework as a whole has yet been finalized or provided to TSA or other sector-specific agencies, it is not

[33] DHS refers to this framework as a Risk Analysis and Management for Critical Asset Protection.

clear what impact, if any, DHS's framework may have on ongoing risk assessments conducted by, and the methodologies used by, TSA, ODP, and others, and whether or how DHS will be able to use these results to compare risks and prioritize homeland security investments among sectors. Until DHS finalizes this framework, and until TSA completes its risk assessment methodology, it may not be possible to determine whether different methodologies used by TSA and ODP for conducting threat, criticality, and vulnerability assessments generate disparate qualitative and quantitative results or how they can best be compared and analyzed. In addition, TSA and others will have difficulty taking into account whether at some point TSA may be unnecessarily duplicating risk management activities already under way at other agencies and whether other agencies' risk assessment methodologies, and the data generated by these methodologies, can be leveraged to complete the assessments required for the transportation sector. In the future, the implementation of DHS's departmentwide proposed reorganization could affect decisions relating to critical infrastructure protection as new directorates are established, such as the directorates of policy and preparedness, and other preparedness assets are consolidated from across the department.

Multiple Federal Agencies Have Taken Actions to Enhance Passenger Rail Security

FTA and FRA were the primary federal agencies involved in passenger rail security matters prior to the creation of TSA. Before and after September 11, these two agencies launched a number of initiatives designed to strengthen passenger rail security. TSA also took steps to strengthen rail security, including issuing emergency security directives to rail operators and testing emerging rail security technologies for screening passengers and baggage. Rail industry stakeholders and federal agency officials raised questions about how effectively DHS had collaborated with them on rail security issues. DHS and DOT have signed a memorandum of understanding intended to identify ways that collaboration with federal and industry stakeholders might be improved.

DOT Agencies Led Initial Efforts to Enhance Passenger Rail Security

Prior to the creation of TSA in November 2001, DOT agencies (i.e., modal administrations)—notably FTA and FRA—were primarily responsible for the security of passenger rail systems. These agencies undertook a number of initiatives to enhance the security of passenger rail systems prior to and after September 11. For example, prior to September 11, FTA offered voluntary security assessments, sponsored training at the Transportation Safety Institute, issued written guidelines to improve emergency response planning, and partially funded a chemical detection demonstration project, called PROTECT, at the Washington Metropolitan Area Transit Authority.

In response to the terrorist attacks on September 11, FTA, using an $18.7 million appropriation by the Department of Defense Emergency Supplemental Act of 2002, launched a multipart transit security initiative, much of which is still in place. The initiative included security assessments, planning, drills, and training, as described below:

- **Security readiness assessments**: FTA deployed teams to assess security at 32 rail transit operators. FTA chose these 32 agencies on the basis of their ridership, vulnerability, and the potential consequences of a terrorist attack. Each assessment included a threat and vulnerability analysis, an evaluation of security and emergency plans, and a focused review of the agency's unified command structure with external emergency responders. FTA completed the assessments in late summer 2002.[34]

- **Security and emergency management technical assistance**: As of July 2005, FTA had provided technical assistance to 32 passenger rail agencies on security and emergency plans and emergency response drills. This is also a follow-on effort to the security assessments, as FTA is helping transit agencies fill identified security gaps customized to the individual agency's needs and operating characteristics.

- **Emergency response drills**: FTA offered transit agencies grants up to $50,000 for organizing and conducting emergency preparedness drills. According to FTA officials, FTA has awarded $3.4 million to over 80 transit agencies through these grants.

- **Transit Safety and Security Roundtables program**: FTA developed the Transit Safety and Security Roundtables program, which brings together safety and security chiefs of the 30 largest transit systems to share information on technology and best practices and to develop relationships between federal and local officials working in the areas of transit safety and security. In October 2003, FTA and DHS, through TSA, sponsored the most recent roundtable, in Washington, D.C. In October 2005, FTA and DHS plan to hold a roundtable with safety and security representatives of the 50 largest transit agencies.

- **Connecting Communities program**: FTA developed and currently is offering free emergency preparedness and security training to transit agencies through its Connecting Communities Forums. These forums are

[34] FTA completed three additional assessments of rail transit agencies as part of its technical assistance program.

designed to bring together personnel from small and medium-sized transit agencies with their local emergency responders, including local firefighters and police officers. The purposes of the forums are to give the participants a better understanding of the roles played by transit agencies and emergency responders and to allow participants to begin developing the plans, tools, and relationships necessary to respond effectively in an emergency. FTA sponsored 17 forums under this program and has plans for the delivery of 12 more by the end of fiscal year 2006. TSA has provided financial support to this program. In fiscal year 2005, TSA transferred $100,000 to FTA to support the Connecting Communities program.

- **Transit Watch program**: In 2003, FTA instituted the Transit Watch campaign, a nationwide safety and security awareness program designed to encourage the active participation of transit passengers and employees in maintaining a safe transit environment. The program provides information and instructions to transit passengers and employees so that they know what to do and whom to contact in the event of an emergency in a transit setting. Transit Watch invites riders and employees to be the "eyes and ears" of their local transit system. FTA plans to continue this initiative, in partnership with TSA and ODP, and offer additional security awareness materials that address unattended bags and emergency evacuation procedures for transit agencies.

- **Additional security training**: In addition to the programs and training cited above, FTA worked with the National Transit Institute, Johns Hopkins University, and the Transportation Safety Institute to expand safety and security course offerings. For example, the National Transit Institute is now offering a security awareness course to frontline transit employees free of charge. The course covers skill sets for observing, determining, and reporting people and items that are suspicious or out of place. FTA also developed a training course for frontline transit employees to recognize and react to terrorist activity. This course incorporates the latest in international counterterrorism techniques.

- **Security guidance**: FTA also developed security guidance for transit agencies based largely on the findings of the security readiness assessments. For example, in November 2003, FTA issued its Top 20 Security Program Action Items for Transit Agencies, which recommends measures for transit agencies to implement into their security programs to improve both security and emergency preparedness. Recommended practices include performing background checks on employees, instituting access control procedures, and providing security awareness training to frontline employees. In 2003, FTA also issued recommended measures for transit agencies to implement in responding to various DHS threat level designations.

FTA has also used research and development funds to develop guidance for security design strategies to reduce the vulnerability of transit systems to acts of terrorism. In November 2004, FTA provided rail operators with security considerations for transportation infrastructure. This guidance provided recommendations intended to help operators deter and minimize attacks against their facilities, riders, and employees by incorporating security features into the design of rail infrastructure. (Additional details on the use of this guidance are discussed later in this report.)

FRA has also taken a number of actions to enhance passenger rail security since September 11. For example, it has assisted commuter railroads in developing security plans, reviewed Amtrak's security plans, and helped fund FTA security readiness assessments for commuter railroads. More recently, in the wake of the Madrid terrorist bombings, nearly 200 FRA inspectors, in cooperation with DHS, conducted multi-day team inspections of each of the 18 commuter railroads and Amtrak to determine what additional security measures had been put into place to prevent a similar occurrence in the United States. FRA also conducted research and development projects related to passenger rail security. These projects included rail infrastructure security and trespasser monitoring systems and passenger screening and manifest projects, including explosives detection.

Although DOT modal administrations now play a supporting role in transportation security matters since the creation of TSA, they remain important partners in the federal government's efforts to improve rail security, given their role in funding and regulating the safety of passenger rail systems. Moreover, as TSA moves ahead with its passenger rail security initiatives, FTA and FRA are continuing their passenger rail security efforts.

TSA Issued Mandatory Security Directives to Rail Operators but Faces Challenges Related to Compliance and Enforcement

In response to the March 2004 commuter rail attacks in Madrid and federal intelligence on potential threats against U.S. passenger rail systems, TSA issued security directives to the passenger rail industry in May 2004. TSA issued these security directives to establish a consistent baseline standard of protective measures for all passenger rail operators, including Amtrak.[35] The directives were not related to, and were issued independent of, TSA's efforts to conduct risk assessments to prioritize rail security needs. TSA considered the measures required by the directives to constitute mandatory security standards that were required to be implemented within 72 hours of issuance by all passenger rail operators nationwide. In an effort to provide some flexibility to the industry, the directives allowed rail operators to propose alternative measures to TSA in order to meet the required measures. Table 3 contains examples of security measures required by these directives.

Table 3: Examples of Measures Required by TSA Security Directives Issued to Passenger Rail Operators and Amtrak

TSA directives require passenger rail operators to:
• designate coordinators to enhance security-related communications with TSA
• provide TSA with access to the latest security assessments and security plans
• reinforce employee watch programs
• ask passengers and employees to report unattended property or suspicious behavior
• remove trash receptacles at stations determined by a vulnerability assessment to be at significant risk and only to the extent practical, except for clear plastic or bomb-resistant containers
• install bomb-resistant trash cans to the extent resources allow
• utilize canine explosive detection teams, if available, to screen passenger baggage, terminals, and trains
• utilize surveillance systems to monitor for suspicious activity, to the extent resources allow
• allow TSA-designated canine teams at any time or place to conduct canine operations
• conduct frequent inspections of key facilities, stations, terminals, or other critical assets for persons and items that do not belong
• inspect each passenger rail car for suspicious or unattended items, at regular periodic intervals
• ensure that appropriate levels of policing and security are provided that correlate to DHS threat levels and threat advisories
• lock all doors that allow access to train operators' cab or compartment, if equipped with locking mechanisms
• require Amtrak to request that adult passengers provide identification at the initial point where tickets are checked

Source: TSA.

Although TSA issued these directives, it is unclear how TSA developed the required measures contained in the directives, how TSA plans to monitor

[35] According to TSA, in issuing the passenger rail and mass transit security directives, TSA exercised its authorities under 49 U.S.C. 114. We are currently examining whether TSA met all relevant legal requirements in the promulgation of the directives.

and ensure compliance with the measures, how rail operators are to implement the measures, and which entities are responsible for their implementation. According to the former DHS Undersecretary for Border and Transportation Security, the directives were developed based upon consultation with the industry and a review of best practices in passenger rail and mass transit systems across the country and were intended to provide a federal baseline standard for security. TSA officials stated to us that the directives were based upon FTA and APTA best practices for rail security. Specifically, TSA stated that it consulted a list of the top 20 actions FTA identified that rail operators can take to strengthen security, FTA-recommended protective measures and activities for transit agencies that may be followed based on current threat levels, and an APTA member survey. While some of the directives correlate to information contained in the FTA guidance, such as advocating that rail personnel watch for abandoned parcels, vehicles, and the like, the source for many of the directives is unclear. For example, the source material TSA consulted does not support the requirement that train cabs or compartment doors should be kept locked. Furthermore, the sources do not necessarily reflect industry best practices, according to FTA and APTA officials. FTA's list of recommended protective measures and the practices identified in the APTA survey are not necessarily viewed as industry best practices. For example, the APTA member survey that TSA used reports rail security practices that are in use by operators but which are not best practices endorsed by the group or other industry stakeholders.

TSA officials have stated that they understood the importance of partnering with the rail industry on security matters, and that they would draw on the expertise and knowledge of the transportation industry and other DHS agencies, as well as all stakeholders, in developing security standards for all modes of transportation, including rail. TSA officials held an initial meeting with APTA, AAR, and Amtrak officials to discuss the draft directives prior to their issuance and told them that they would continue to be consulted prior to their final issuance. However, these stakeholders were not given an opportunity to comment on a final draft of the directives before their release because, according to TSA, DHS determined that it was important to release the directives as soon as possible to address a current threat to passenger rail. In addition, TSA stated that because the directives needed to be issued quickly, there was no public comment as part of the rule-making process. Shortly after the directives were issued, TSA's Deputy Assistant Administrator for Maritime and Land Security told rail operators at an APTA conference we attended in June 2004 that if TSA determined that there is a need for the directives to become permanent, they would undergo a notice-and-comment period as part of the regulatory process. As of July 2005, TSA had not yet determined whether it intends to pursue the rule-making process with a notice-and-comment period.

APTA and AAR officials stated that because they were not consulted throughout the development of the directives, the directives did not, in their view, reflect a complete understanding of the passenger rail environment or necessarily incorporate industry best practices. For example, APTA, AAR, and some rail operators raised concerns about the feasibility of installing bomb-resistant trash cans in rail stations because they could direct the force of a bomb blast upward, possibly causing structural damage in underground or enclosed stations. DHS's Office for State and Local Government Coordination and Preparedness recently conducted tests to determine the safety and effectiveness of 13 models of commercially available bomb-resistant trash receptacles. At the time of our review, the results of these tests were not yet available.

Amtrak and FRA officials raised concerns about some of the directives, as well, and told us they questioned whether the requirements reflected industry best practices. For example, before the directives were issued, Amtrak expressed concerns to TSA about the feasibility of the requirement to check the identification of all adult passengers boarding its trains because they did not have enough staff to perform these checks. However, the final directive included this requirement, and after they were released, Amtrak told TSA it could not comply with this requirement "without incurring substantial additional costs and significant detrimental impacts to its operations and revenues." Amtrak officials told us that since passenger names would not be compared against any criminal or terrorist watch list or database, the benefits of requiring such identification checks were open to debate. To resolve its concern, and as allowed by the directive, Amtrak proposed, and TSA accepted, random identification checks of passengers as an alternative measure. FRA officials further stated that current FRA safety regulations requiring engineer compartment doors be kept unlocked to facilitate emergency escapes[36] conflicts with the security directive requirement that doors equipped with locking mechanisms be kept locked. This requirement was not included in the draft directives provided to stakeholders. TSA did call one commuter rail operator prior to issuing the directives to discuss this potential proposed measure, and the operator raised a concern about the safety of the locked

[36] 49 CFR 238.235.

door requirement. TSA nevertheless included this requirement in the directives.

With respect to how the directives were to be enforced, rail operators were required to allow TSA and DHS to perform inspections, evaluations, or tests based on execution of the directives at any time or location. Upon learning of any instance of noncompliance with TSA security measures, rail operators were to immediately initiate corrective action. Monitoring and ensuring compliance with the directives has posed challenges for TSA. In the year after the directives were issued, TSA did not have dedicated field staff to conduct on-site inspections. When the rail security directives were issued, the former DHS Undersecretary for Border and Transportation Security stated that TSA planned to form security partnership teams with DOT, including FRA rail inspectors, to help ensure that industry stakeholders complied with the directives. These teams were to be established in order to tap into existing capabilities and avoid duplication of effort across agencies. As of July 2005, these teams had not yet been utilized to perform inspections. TSA has, however, hired rail compliance inspectors to, among other things, monitor and enforce compliance with the security directives. As of July 2005, TSA had hired 57 of up to 100 inspector positions authorized by Congress.[37] However, TSA has not yet established processes or criteria for determining and enforcing compliance, including determining how rail inspectors or DOT partnership teams will be used in this regard.

Establishing criteria for monitoring compliance with the directives may be challenging because the language describing the required measures allows for flexibility and does not define parameters. In an effort to acknowledge the variable conditions that existed in passenger rail environments, TSA designed the directives to allow flexibility in implementation through the use of such phrases as “to the extent resources allow,” “to the extent practicable,” and “if available.” The directives also include non-specific instructions that may be difficult to measure or monitor, telling operators to, for example, perform inspections of key facilities at “regular periodic intervals” or to conduct “frequent inspections” of passenger rail cars. When the directives were issued, TSA stated that it would provide rail operators with performance-based guidance and examples of

[37] These positions were funded through the DHS Appropriations Act of 2005 and its accompanying conference report, which provided TSA with $12 million in funding for rail security activities.

announcements and signs that could be used to meet the requirements of the directives, including guidance on the appropriate frequency and method for inspecting rail cars and facilities. However, as of July 2005, this information had not been provided.

Industry stakeholders we interviewed raised questions about how they were to comply with the measures contained in the directives and which entities were responsible for implementing the measures. According to an AAR official, in June 2004, AAR officials and rail operators held a conference call with TSA to obtain clarification on these issues. According to AAR officials, in response to an inquiry about what would constitute compliance for some of the measures, the then-TSA Assistant Administrator for Maritime and Land Security told participants that the directives were not intended to be overly prescriptive but were guidelines, and that operators would have the flexibility to implement the directives as they saw fit. The officials also asked for clarification on who was legally responsible for ensuring compliance for measures where assets, such as rail stations, were owned by freight railroads or private real estate companies. According to AAR officials, TSA told them it was the responsibility of the rail operators and asset owners to work together to determine these responsibilities. However, according to AAR and rail operators, given that TSA has hired rail inspectors and indicated its intention to enforce compliance with the directives, it is critical that TSA clarify what compliance entails for measures required by the directives and which entities are responsible for compliance with measures when rail assets are owned by one party but operated by another—such as when private companies that own terminals or stations provide services for commuter rail operations.

The challenges TSA has faced in developing security directives as standards that reflect industry best practices—and which can be measured and enforced—stem from the original emergency nature of the directives, which were issued with limited input and review. TSA told rail industry stakeholders when the directives were issued 15 months ago that the agency would consider using the federal rule-making process as a means of making the standards permanent. Doing so would require TSA to hold a notice-and-comment period, resulting in a public record that reflects stakeholders' input on the applicability and feasibility of implementing the directives, along with TSA's rationale for accepting or rejecting this input. While there is no guarantee that this process would produce more effective security directives, it would be more transparent and could help TSA in developing standards that are most appropriate for the industry and can be measured, monitored, and enforced.

TSA Has Begun Testing Rail Security Technologies

In addition to issuing security directives, TSA also sought to enhance passenger rail security by conducting research on technologies related to screening passengers and checked baggage in the passenger rail environment. Beginning in May 2004, TSA conducted a Transit and Rail Inspection Pilot (TRIP) study, in partnership with DOT, Amtrak, the Connecticut Department of Transportation, the Maryland Transit Administration, and the Washington Metropolitan Area Transit Authority (WMATA). TRIP was a $1.5 million, three-phase effort to test the feasibility of using existing and emerging technologies to screen passengers, carry-on items, checked baggage, cargo, and parcels for explosives. Figure 5 summarizes TRIP's three-phased approach.

Figure 5: Summary Information on TSA's Transit and Rail Inspection Pilot Program Phases

Phase I: Screen commuter rail passengers and carry-on baggage before trains are boarded using an explosive detection device similar in appearance to an airport metal detector and other explosive screening technologies.

Phase II: Screen passenger baggage including checked baggage, unclaimed baggage, and cargo on long-haul Amtrak trains prior to departure.

Phase III: Screen passengers and their carry-on baggage on board a moving commuter rail train. All passengers are required to enter the train in the specially designed screening car, which was a commuter rail passenger car that been reconfigured to hold screening equipment and security personnel.

Source: TSA.

According to TSA, all three phases of the TRIP program were completed by July 2004. However, TSA has not yet issued a planned report analyzing whether the technologies could be used effectively to screen rail passengers and their baggage. According to TSA officials, a report on results and lessons learned from TRIP is under review by DHS. TSA officials told us that based upon preliminary analyses, the screening technologies and processes tested would be very difficult to implement on more heavily used passenger rail systems, such as mass transit systems in large urban areas, because these systems carry high volumes of passengers and have multiple points of entry. However, TSA officials stated to us that the screening processes used in TRIP may be useful on certain long-distance intercity train routes, which make fewer stops. Further, officials stated that screening could be used either randomly or for all passengers during certain high-risk events or in areas where a particular terrorist threat is known to exist. For example, screening technology similar to that used in TRIP was used by TSA to screen certain passengers and belongings in Boston and New York during the Democratic and Republican national conventions, respectively, in 2004.

APTA officials and the 28 passenger rail operators we interviewed—all who are not directly involved in the pilot—agreed with TSA's preliminary assessment. They told us they believed that the TRIP screening procedures could not work in most passenger rail systems, given the number of passengers using these systems and the open nature (e.g., multiple entry points) of the systems. For example, as one operator noted, over 1,600 people pass through dozens of access points in New York's Penn Station per minute during a typical rush hour, making screening of all passengers very challenging, if not impossible. Passenger rail operators were also concerned that screening delays could result in passengers opting to use other modes of transportation. APTA officials and some rail operators we interviewed said that had they been consulted by TSA, they would have recommended alternative technologies to explore and indicated that they hoped to be consulted on security technology pilot programs in the future. FRA officials further stated that TSA could have benefited from earlier and more frequent collaboration with them during the TRIP pilot than occurred, and could have tapped their expertise to analyze TRIP results and develop the final report. TSA research and development officials told us that the agency has begun to consider and test security technologies other than those used in TRIP, which may be more applicable to the passenger rail environment. For example, TSA's and DHS's Science and Technology Directorate are currently evaluating infrared cameras and electronic metal detectors, among other things.

DHS and DOT Are Taking Steps to Improve Coordination and Collaboration with Federal Agencies and Industry Stakeholders

In our prior transportation security work, we have called for improved coordination among all levels of government and the private sector, as a means of enhancing security across all transportation modes.[38] In September 2004, DHS and DOT signed a memorandum of understanding to develop procedures by which the two departments could improve their cooperation and coordination for promoting the safe, secure, and efficient movement of people and goods throughout the transportation system. The MOU defines broad areas of responsibility for each department. For example, it states that DHS, in consultation with DOT and affected stakeholders, will identify, prioritize, and coordinate the protection of

[38] GAO-03-263 and GAO-03-843.

critical infrastructure. The MOU was developed in response to a recommendation we made in June 2003 in which we noted that the roles and responsibilities of DOT and TSA for transportation security matters had not been clearly defined. We emphasized the need for greater coordination between DOT and TSA on transportation security efforts—noting that the lack of coordination can lead to duplication or conflicting efforts and gaps in preparedness. To improve coordination between DOT and DHS on transportation security matters, we recommended that DOT and DHS develop a mechanism, such as a memorandum, to clearly define roles and responsibilities for transportation security matters, in such areas as the development and implementation of security standards and regulations, determining funding priorities, and interfacing with the transportation industry.

The MOU between DHS and DOT represents an overall framework for cooperation that is to be supplemented by additional signed agreements, or annexes, between the departments. These annexes are to delineate the specific security-related roles, responsibilities, resources, and commitments for mass transit, rail, research and development, and other matters. As of July 2005, separate annexes for mass transit security, rail security, and research and development were at various stages of development, according to DHS and DOT officials. DHS and DOT officials told us that an annex for mass transit security had been prepared and was undergoing final review by both departments. According to DHS and DOT officials, the annex is intended to ensure that the programs and protocols for incorporating stakeholder feedback and making enhancements to security measures are coordinated.

According to officials, the mass transit annex will address how DHS's Office of State and Local Government Coordination and Preparedness, TSA, FTA, and DOT's Office of Intelligence, Security, and Emergency Management are to coordinate their programs and services, including grants, training, exercises, risk assessments, and technical assistance, in order to better assist transit agencies in prioritizing and addressing their security needs. For example, officials stated to us that the annex would likely address coordination on such programs as FTA's Transit Watch and Transit Safety and Security Roundtables programs, which are designed to raise transit employees' on-the-job awareness about security and provide a forum for stakeholders to share information on technology and best practices. In addition, according to officials, the annex will require DHS and DOT to consult on such matters as regulations and security directives that affect security and will identify points of contact for coordinating this consultation.

In addition to the annexes currently under development, DHS and DOT must also complete an annex to define and clarify the respective roles and responsibilities of DHS and DOT relating to public transportation security within 45 days of the enactment of The Safe, Accountable, Flexible, and Efficient Transportation Equity Act of 2005, which President Bush signed on August 10, 2005. According to the law, this annex shall establish a process to develop security standards for public transportation agencies; create a method of direct coordination with public transportation agencies on security matters; address any other issues determined to be appropriate by the Secretary of Transportation and the Secretary of Homeland Security; and include a formal and permanent mechanism to ensure coordination and involvement by DOT, as appropriate, in public transportation security.[39]

In addition to their work on the MOU and related annexes, DHS and TSA have taken other steps in an attempt to improve collaboration with DOT and industry stakeholders. In April 2005, DHS officials stated that better collaboration with DOT and industry stakeholders was needed to develop strategic security plans associated with various homeland security presidential directives and statutory mandates, such as the Intelligence Reform and Terrorism Prevention Act of 2004, which required DHS to develop a national strategy for transportation security in conjunction with DOT. Responding to the need for better collaboration, DHS established a senior-level steering committee in conjunction with DOT to coordinate development of this national strategy. In addition, senior DHS and TSA officials stated that industry groups will also be involved in developing the national strategy for transportation security and other strategic plans. Moreover, according to TSA's assistant administrator for intermodal programs, TSA intends to work with APTA and other industry stakeholders in developing security standards for the passenger rail industry.[40]

[39] Section 3028 of Pub. L. No. 109-59.

[40] APTA is a standards development organization recognized by DOT that has set standards for commuter rail, mass transit, and bus safety and operations.

U.S. and Foreign Rail Operators Have Taken Similar Actions to Secure Rail Systems, and Opportunities for Additional Domestic Security Actions May Exist

U.S. passenger rail operators have taken numerous actions to secure their rail systems since the terrorist attacks of September 11, in the United States, and the March 11, 2004, attacks in Madrid. These actions included both improvements to system operations and capital enhancements to a system's facilities, such as track, buildings, and train cars. All of the U.S. passenger rail operators we contacted have implemented some types of security measures—such as increased numbers and visibility of security personnel and customer awareness programs—that were generally consistent with those we observed in select countries in Europe and Asia. We also identified three rail security practices—covert testing, random screening of passengers and their baggage, and centralized research and testing—utilized by foreign operators or their governments that are not currently utilized by domestic rail operators or the U.S. government.[41]

Actions Taken by U.S. and Foreign Passenger Rail Operators to Strengthen Security Reflect Security Assessments, Budgetary Constraints, and Other Factors

All 32 of the U.S. rail operators we interviewed or visited reported taking specific actions to improve the security and safety of their rail systems by, among other things, investing in new security equipment, utilizing more law enforcement personnel, and establishing public awareness campaigns. Passenger rail operators we spoke with cited the 1995 sarin gas attacks on the Tokyo subway system and the September 11 terrorist attacks as catalysts for their security actions. After the attacks, many passenger rail operators used FTA's security readiness assessments of heavy and passenger rail systems as a guide to determine how to prioritize their security efforts, as well as their own understanding of their system's vulnerabilities, to determine what actions to take to enhance security. Similarly, as previously mentioned, the rail systems that underwent ODP risk assessments are currently using or plan to use these assessments to guide their security actions. In addition, 20 of the 32 U.S. operators we contacted or visited had conducted some type of security assessment internally or through a contractor, separate from the federally funded assessments. For example, some assessments evaluated vulnerabilities of physical assets, such as tunnels and bridges, throughout the passenger rail system. Passenger rail operators stated that security-related spending by rail operators was also based, in part, on budgetary considerations, as well as other practices used by other rail operators that were identified through

[41] At the time we completed our work, in June 2005, these three practices were not utilized. However, as discussed later in this report, some rail operators began using random screening in the aftermath of the July bomb attacks on the London subway system.

direct contact or during industry association meetings.[42] Passenger rail operators frequently made capital investments to improve security, and these investments often are not part of federal funding packages for new construction unless they are part of new facilities being constructed. According to APTA, 54 percent of transit agencies are facing increasing deficits, and no operator covers expenses with fare revenue; thus, balancing operational and capital improvements with security-related investments has been an ongoing challenge for these operators. Several foreign rail operators we interviewed also stated that funding for security enhancements was limited in light of other funding priorities within the rail system, such as personnel costs and infrastructure and equipment maintenance.

Foreign rail operators we visited also told us that risk assessments played an important role in guiding security-related spending for rail. For example, one foreign rail operator with a daily ridership of 2.3 million passengers used a risk management methodology to assess risks, threats, and vulnerabilities to rail in order to guide security spending. The methodology is part of the rail operator's corporate focus on overall safety and security and is intended to help protect the operator's various rail systems against, among other things, terrorist attacks, as well as other forms of corporate loss, such as service disruption and loss of business viability. According to the operator, the methodology employs a "risk-informed" approach to support management's business decision process regarding security. Other than the results of risk assessments, issues such as laws and regulations, and business requirements, are also taken into consideration. The approach relies on a combination of risk, threat, and vulnerability assessment and management, and focuses on proactive prevention. Implementing the methodology involves all corporate departments and staff at three activity levels:

- At the corporate level, the focus on security is articulated in a three-part corporate security policy that states, among other things, that managers are responsible for performing risk management activities in their functional areas and maintaining cost-effective security measures.

[42] As we have previously reported, since the mid-1990s, federal funding for transit and commuter rail operators has generally been limited to assistance with capital projects involving building new transit service, extensions of existing lines, or rehabilitation of existing transit infrastructure, such as tracks, rolling stock, or stations. See GAO-03-263.

- At the department level, department heads are responsible for promoting security awareness, setting rules and guidelines, and allocating security responsibilities (in the form of assigning "risk ownership").

- At the line level, managers are responsible for implementing the risk assessment component of the methodology, consistent with the security policy described earlier. This component, which involves an iterative process, consists of identifying threats and quantifying risks (risk is expressed as a function of likelihood and consequence); designing and implementing security protective measures; and measuring compliance with and the effectiveness of these measures, similar to our risk management approach.

According to officials of the foreign rail operator, to measure performance, the operator conducts periodic surveys to measure the perceptions of riders and employees; rates the success of drills; and measures the incidence of crime (such as pick pocketing). The operator's security department also conducts audits to measure compliance and help ensure that security procedures are being followed. Separately, the rail operator's insurers review the security management of the rail system, including the methodology, every 4 years.

U.S. and Foreign Rail Operators Employ Similar Security Practices

Both U. S. and foreign passenger rail operators we contacted have implemented similar operational and capital improvements[43] to enhance the security of their systems.[44] A summary of these efforts follows.

Operational improvements

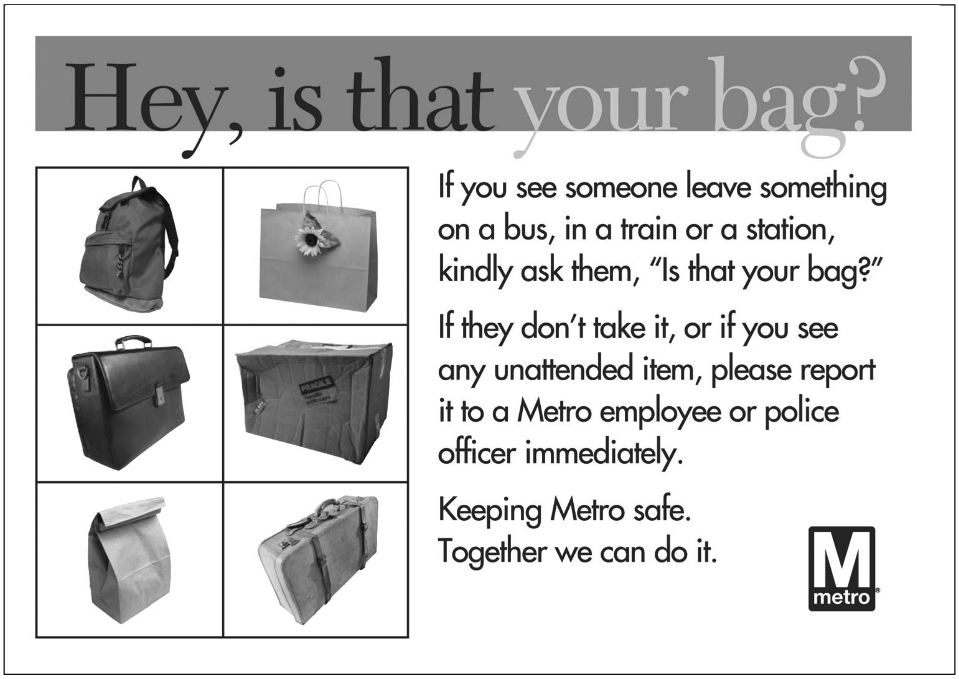
Customer awareness: Customer awareness programs we observed used signage and announcements to encourage riders to alert train staff if they observed suspicious packages, persons, or behavior. Of the 32 domestic rail operators we interviewed, 30 had implemented a customer awareness program or made enhancements to an existing program. FTA has assisted

[43] Operational enhancements are actions that involve changes to the way a rail agency's staff operate their rail system on a day-to-day basis—such as enhancing customer awareness, increasing the number and visibility of security personnel, training employees, and implementing selective passenger and baggage screening. Capital improvements include construction of new facilities or rehabilitation of old facilities such as stations, train yards, tracks, and so on, or purchase of new equipment to enhance existing capabilities.

[44] Actions taken by Amtrak to enhance security are discussed later in this report.

rail operators in this area by creating the Transit Watch program, in cooperation with industry groups such as APTA. Transit Watch is a nationwide safety and security awareness program designed to encourage the active participation of transit passengers and employees in maintaining a safe transit environment. FTA distributed education and training materials to rail operators so these materials could be provided to customers and employees. Rail operators stated that they attempt to entitle their customer awareness programs so that customers can easily remember the goals of the program. New York City Transit's "If You See Something, Say Something" campaign and the WMATA program, "Is That Your Bag?" are examples of this. (See fig. 6 for an example of public awareness signage). Foreign rail operators we visited also attempt to enhance customer awareness. For example, 11 of the 13 operators we interviewed had implemented a customer awareness program. Similar to programs of U.S. operators, these programs used signage, announcements, and brochures to inform passengers and employees about the need to remain vigilant and report any suspicious activities. Only one of the European passenger rail operators that we interviewed has not implemented a customer security awareness program, citing the fear or panic that it might cause among the public.

Figure 6: Example of Passenger Rail Customer Awareness Poster



Hey, is that your bag?

If you see someone leave something on a bus, in a train or a station, kindly ask them, "Is that your bag?"

If they don't take it, or if you see any unattended item, please report it to a Metro employee or police officer immediately.

Keeping Metro safe.
Together we can do it.

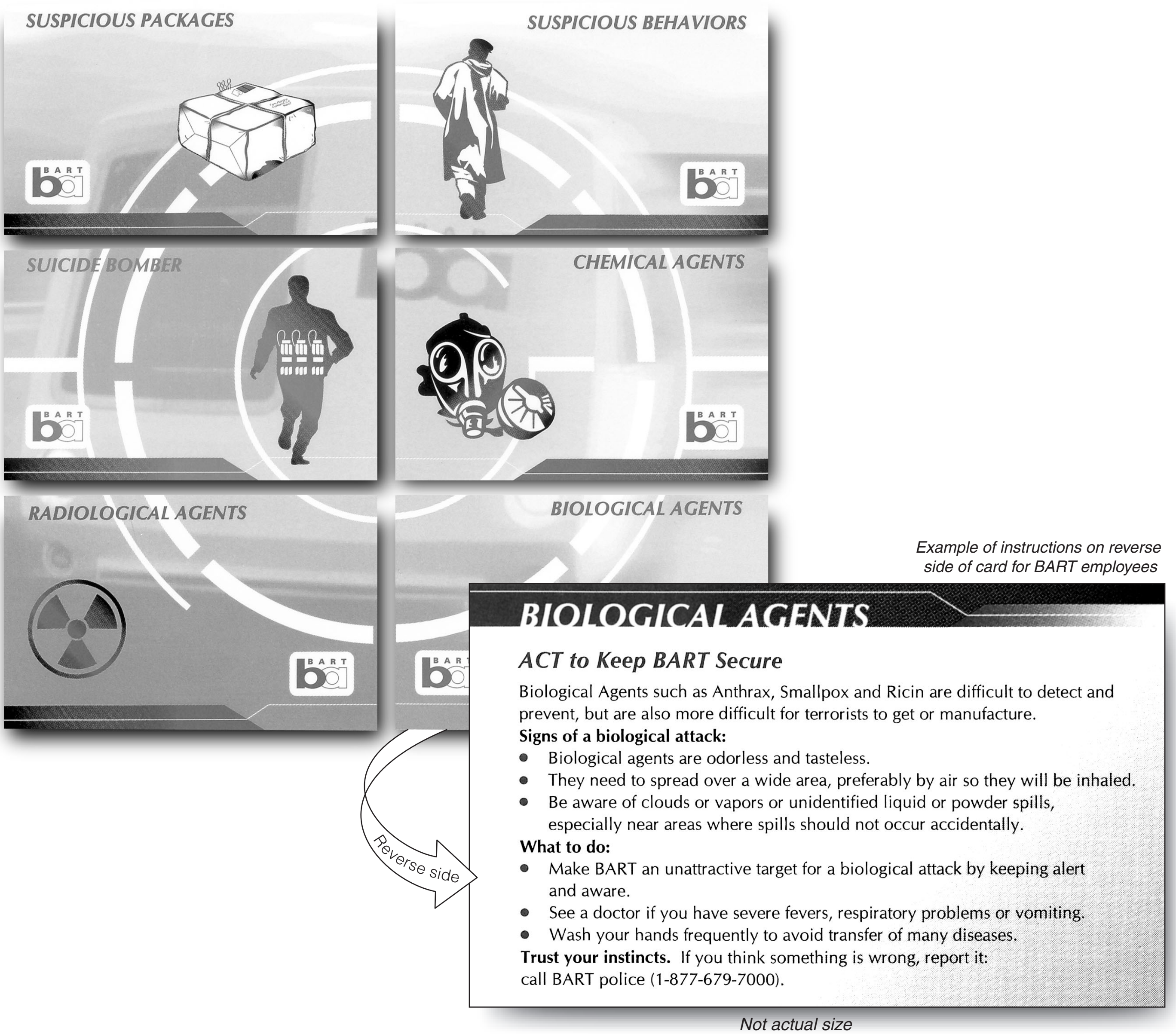
Source: WMATA.

Increased number and visibility of security personnel: Of the 32 U.S. rail operators we interviewed, 23 had increased the number of security personnel they utilized since September 11, to provide security throughout their system or had taken steps to increase the visibility of their security personnel. In addition to adding security personnel, many operators stated that increasing the visibility of security was as important as increasing the number of personnel. For example, several U.S. and foreign rail operators we spoke with had instituted policies such as requiring their security staff, in brightly colored vests, to patrol trains or stations more frequently, so they are more visible to customers and potential terrorists or criminals. These policies make it easier for customers to contact security personnel in the event of an emergency, or if they have spotted a suspicious item or person. At foreign sites we visited, 10 of the 13 operators had increased the number of their security officers throughout their systems in recent years because of the perceived increase in risk of a terrorist attack. One rail operator, the Tokyo Metro system, in addition to increasing the number of security personnel, has also made them more visible. Tokyo Metro stations now include an elevated security platform for security personnel to stand on, which allows them to better see throughout the station and allows passengers to see the security staff more easily.

Increased use of canine teams: Of the 32 U.S. passenger rail operators we contacted, 21 had begun to use canine units, which include both dogs and human handlers, to patrol their facilities or trains or had increased their existing utilization of such teams. Often, these units are used to detect the presence of explosives, or in some cases, drugs, and may be called in when a suspicious package is detected. One operator we spoke with uses its canines to patrol its system simply as a crime deterrent rather than to detect explosives or drugs. Some operators that did not maintain their own canine units stated that it was prohibitively expensive to do so and that they could call in local police canine units if necessary. In foreign countries we visited, passenger rail operators' use of canines varied. In some Asian countries, canines were not culturally accepted by the public and thus were not used for rail security purposes. In contrast, most European passenger rail operators, as in the United States, used canines for explosive detection or as deterrents.

Employee training: All of the domestic and foreign rail operators we interviewed had provided some type of security training to their staff, either through in-house personnel or an external provider. In many cases, this training consisted of ways to identify suspicious items and persons and how to respond to events once they occur. For example, the London Underground and the British Transport Police developed the "HOT" method for its employees to identify suspicious items in the rail system. In the HOT method, employees are trained to look for packages or items that are *Hidden*, *Obviously* suspicious, and not *Typical* of the environment. Items that do not meet these criteria would likely receive a lower security response than an item meeting all of the criteria. However, if items meet all of these criteria, employees are to notify station managers, who would call in the authorities and potentially shut down the station or take other action. According to London Underground officials, the HOT method has significantly reduced the number of system disruptions caused when a suspicious item was identified. In addition, officials noted that the HOT method is easy for rail employees to remember and is successful, in part, because it provides rail employees with the discretion to make security-related decisions on their own. According to British Transport Police and London Underground officials, there have been no cases where unattended packages that employees determined did not meet the HOT criteria contained explosive devices. Several passenger rail operators in the United States and abroad have trained their employees in the HOT method. Several domestic operators had also trained their employees in how to respond to terrorist attacks and provided them with wallet-size cards highlighting actions they should take in response to various forms of attack. (See fig. 7 for examples of cards that are distributed by the San Francisco Bay Area Rapid Transit [BART] to their employees to help them prevent or respond to terrorist attacks.) It is important to note that training such as the HOT method is not designed to prevent acts of terrorism like the July 2005 London attacks, where suicide bombers killed themselves rather than leaving bombs behind.

Figure 7: Wallet-size Cards Distributed to BART Employees Containing Anti-terrorism Information



Example of instructions on reverse side of card for BART employees

BIOLOGICAL AGENTS

ACT to Keep BART Secure

Biological Agents such as Anthrax, Smallpox and Ricin are difficult to detect and prevent, but are also more difficult for terrorists to get or manufacture.

Signs of a biological attack:

- Biological agents are odorless and tasteless.
- They need to spread over a wide area, preferably by air so they will be inhaled.
- Be aware of clouds or vapors or unidentified liquid or powder spills, especially near areas where spills should not occur accidentally.

What to do:

- Make BART an unattractive target for a biological attack by keeping alert and aware.
- See a doctor if you have severe fevers, respiratory problems or vomiting.
- Wash your hands frequently to avoid transfer of many diseases.

Trust your instincts. If you think something is wrong, report it: call BART police (1-877-679-7000).

Not actual size

Source: San Francisco Bay Area Rapid Transit District.

Officials from the London Underground also provided insights into the importance of how training is provided to staff, in addition to the type of training provided. In training rail station staff, London Underground officials stressed the importance of direct supervisors or managers providing security briefings to each employee or small groups of employees. In doing so, officials stated that they believed it helps make staff more aware of their responsibilities in certain situations, enables supervisors to hold employees accountable for what they learned in training, and allows employees to ask questions related to their specific job duties.

Passenger and baggage screening practices: Some domestic and foreign rail operators have trained employees to recognize suspicious behavior as a means of screening passengers. Eight U.S. passenger rail operators we contacted were utilizing some form of behavioral screening. For example, the Massachusetts Bay Transportation Authority (MBTA), which operates Boston's T system, has utilized a behavioral screening system to identify passengers exhibiting suspicious behavior. The Massachusetts State Police train all MBTA personnel to be on the lookout for behavior that may indicate someone has criminal intent, and to approach and search such persons and their baggage when appropriate. Massachusetts State Police officers have been training rail operators on this behavior profiling system, and WMATA and New Jersey Transit were among the first additional operators to implement the system. According to MBTA personnel, several other operators have expressed interest in this system. Abroad, we found that 4 of 13 operators we interviewed had implemented forms of behavioral screening similar to MBTA's system. (Rail operators' use of random screening of passengers is discussed later in the report.)

All of the domestic and foreign rail operators we contacted have ruled out an airport-style screening system for daily use in heavy traffic, where each passenger and the passenger's baggage are screened by a magnetometer or X-ray machine, based on cost, staffing, and customer convenience factors, among others. For example, although the Spanish National Railway screens passenger baggage using an X-ray machine on certain long-distance trains that it believes could be at risk, all of the operators we contacted stated that the cost, staffing requirements, delay of service, and inconvenience to passengers would make such a system unworkable in highly trafficked, inherently open systems like U.S. and foreign passenger rail operations. In addition, one Asian rail official stated that his organization was developing a contingency plan for implementing an airport-style screening system, but that such a system would be used only in the event of intelligence information indicating suicide bomb attacks were imminent, or if several attacks had already occurred during a short period of time. According to this official, the plan was in the initial stages of development, and the organization did not know how quickly such a system could be implemented.

Capital improvements

Upgrading technology: Many rail operators we interviewed had embarked on programs designed to upgrade their existing security technology. For example, we found that 29 of the 32 U.S. operators had implemented a form of CCTV to monitor their stations, yards, or trains. While these cameras cannot be monitored closely at all times, because of the large number of staff they said this would require, many rail operators felt the cameras acted as a deterrent, assisted security personnel in determining how to respond to incidents that have already occurred, and could be monitored if an operator has received information that an incident may occur at a certain time or place in their system. One rail operator, New Jersey Transit, had installed "smart" cameras, which were programmed to alert security personnel when suspicious activity occurred, such as if a passenger left a bag in a certain location or if a boat were to dock under a bridge. According to the New Jersey Transit officials, this technology was relatively inexpensive and not difficult to implement. Several other operators stated they were interested in exploring this technology.

Abroad, all 13 of the foreign rail operators we visited had CCTV systems in place. For example, the London Underground uses an extensive system of CCTV cameras to monitor all of its passenger rail system stations and respond to both criminal and emergency incidents. In addition, one Asian system we visited had over 1,000 cameras recording activity in some of its busier stations. However, as in the United States, foreign rail operators use these cameras primarily as a crime deterrent and to respond to incidents after they occur, because they do not have enough staff to continuously monitor all of these cameras. The Madrid Metro is currently testing the use of personal digital assistants (PDA), which would have the ability to operate all security functions in passenger rail stations. These PDAs would enable security staff to monitor any station CCTV camera that they chose from the PDA and respond to a potential emergency, such as a terrorist attack, by shutting down rail or station operations (escalators or ventilation systems, amongst others) from the PDA itself. Madrid Metro officials said that they plan to make the use of the PDAs operational in the future, but did not know when they would do so.

In addition, 18 of the 32 U.S. rail operators we interviewed had installed new emergency phones or enhanced the visibility of the intercom systems they already had. Passengers can use these systems to contact train operators or security personnel to report suspicious activity, crimes in progress, or other problems. Furthermore, while most rail operators we spoke with had not installed chemical or biological agent detection equipment because of the costs involved, a few operators had this equipment or were exploring purchasing it. For example, WMATA, in Washington, D.C., has installed these sensors in some of its stations, thanks to a program jointly sponsored by DOT and the Department of Energy that provided this equipment to WMATA because of the high perceived likelihood of an attack in Washington, D.C. Also, at least three other domestic rail operators we spoke with are exploring the possibility of partnering with federal agencies to install such equipment in their facilities on an experimental basis.

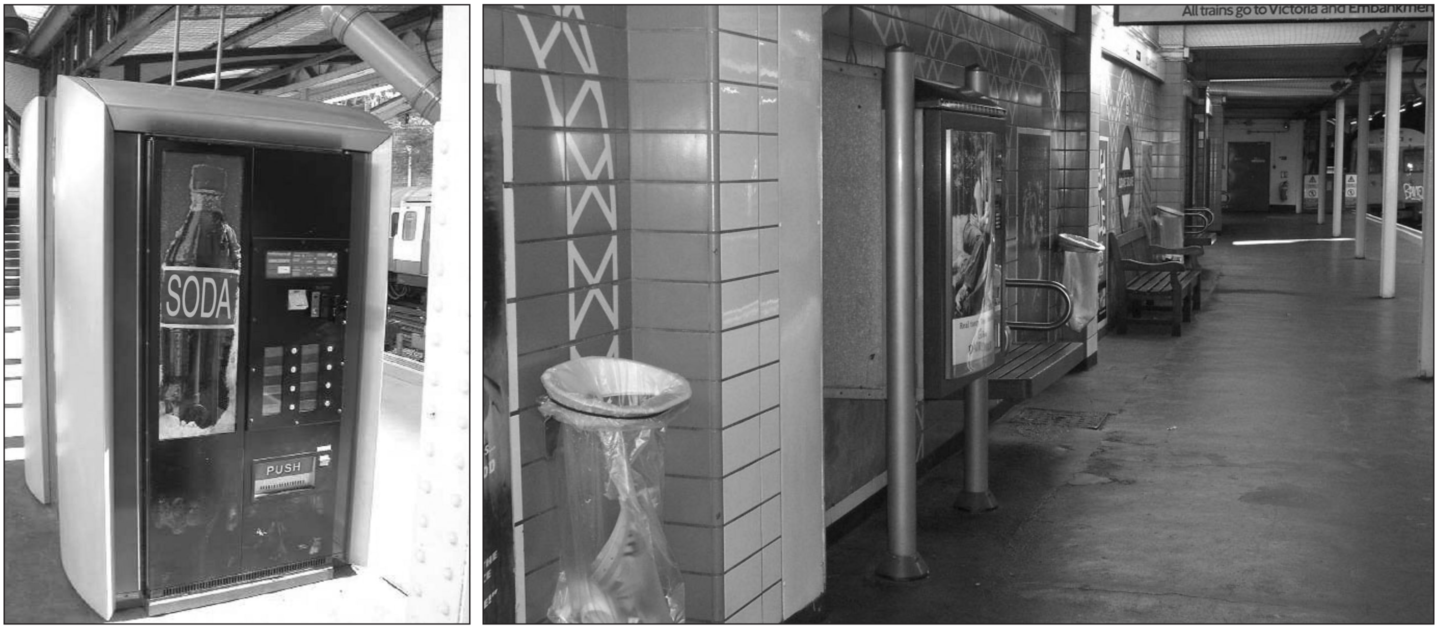
Also, as in the United States, a few foreign operators had implemented chemical or biological detection devices at these rail stations, but their use was not widespread. Two of the 13 foreign operators we interviewed had implemented these sensors, and both were doing so on an experimental basis. In addition, police officers from the British Transport Police—responsible for policing the rail system in the United Kingdom—were equipped with pagers to detect chemical, biological, or radiological elements in the air, allowing them to respond quickly in case of a terrorist attack using one of these methods. The British Transit Police also has three vehicles carrying devices to determine if unattended baggage contains explosives—these vehicles patrol the system 24 hours per day.

Access control: Tightening access procedures at key facilities or rights-of-way is another way many rail operators have attempted to enhance security. A majority of domestic and selected foreign passenger rail operators had invested in enhanced systems to control unauthorized access at employee facilities and stations. Specifically, 23 of the 32 U.S. operators had installed a form of access control at key facilities and stations. This often involved installing a system where employees had to swipe an access card to gain access to control rooms, repair facilities, and other key locations. For example, the Greater Cleveland Regional Transit Authority had a particularly comprehensive system where all doors throughout its rail system are linked to a central alarm and intrusion detection system. If an unauthorized employee or customer attempts to gain access to any facility system wide, alarms are to activate in the control center. Also, BART in California has a modern system utilizing lasers to detect intruders at tunnel portals and other key facilities. Finally, all 13 foreign operators had implemented some form of access control to their critical facilities or rights-of-way. However, these measures varied from simple alarms on doors at electrical substations on one subway system we visited to infrared sensors monitoring every inch of right-of-way along the track on three of the high-speed interurban rail systems. The high-speed systems had these extensive systems because of the potential for catastrophe if a train traveling at over 200 miles per hour were to hit a vehicle placed along the tracks or travel over rail that had been sabotaged.

Rail system design and configuration: In an effort to reduce vulnerabilities to terrorist attack and increase overall security, passenger rail operators in the United States and abroad have been, or are now beginning to, incorporate security features into the design of new and existing rail infrastructure, primarily rail stations. For example, of the 32 domestic rail operators we contacted, 22 of them had removed their conventional trash bins entirely, or replaced them with transparent or bomb-resistant trash bins, as TSA instructed in its May 2004 security directives. In past terrorist attacks on rail systems, particularly in Great Britain, trash bins have been used as a means for hiding explosive devices. Removing trash bins entirely, as PATH in New Jersey has done, eliminates the trash bin as a place to hide an explosive device. Installing transparent trash bins, as a few operators have done, might allow security personnel to see inside trash bins to determine if suspicious items are inside. Three operators have installed bomb-resistant trash bins to contain the impact of a blast and minimize the amount of dangerous shrapnel that could be expelled. Conversely, one rail operator told us that his agency was not removing any of its conventional trash bins because it feared litter would become an unmanageable problem without them and that bomb-resistant and transparent trash bins were ineffective—specifically, that they simply directed the force of a bomb blast upward toward the ceiling, which could cause severe structural damage in an underground station. Similarly, while only a limited number of domestic rail operators we contacted ever had bicycle or storage lockers in their systems, many of those operators that did, at one time, have those lockers told us that they had removed them to avoid the possibility of someone using them as a hiding place for an explosive, or had moved them to locations farther away from stations and crowded places to minimize the impact of a potential attack. Also, foreign rail operators had taken steps to remove traditional trash bins from their systems. Of the 13 operators we visited, 8 had either removed their trash bins entirely or replaced them with blast-resistant cans or transparent receptacles. In fact, the London Underground rail system was the first system worldwide to begin using clear plastic trash bags to eliminate places to hide an explosive. Officials from the Underground stated that this technique helped to deter terrorists from the Irish Republican Army from placing bombs in conventional trash cans during the height of that organization's terrorist campaign against the rail system.

Many foreign rail operators are also incorporating aspects of security into the design of their rail infrastructure. Of the 13 operators we visited, 11 have attempted to design new facilities with security in mind and have attempted to retrofit older facilities to incorporate security-related modifications. For example, one foreign operator we visited is retrofitting its train cars with windows that passengers could open in the event of a chemical attack. In addition, the London Underground, one of the oldest rail systems in the world, incorporates security into the design of all its new stations as well as when existing stations are modified. We observed several security features in the design of Underground stations, such as using vending machines that have no holes that someone could use to hide a bomb, and sloped tops to reduce the likelihood that a bomb can be placed on top of the machine. In addition, stations are designed to provide staff with clear lines of sight to all areas of the station, such as underneath benches or ticket machines, and station designers try to eliminate or restrict access to any recessed areas where a bomb could be hidden. Figure 8 shows selected security design elements incorporated into London Underground stations.

Figure 8: Selected Security Design Elements Incorporated into London's Underground

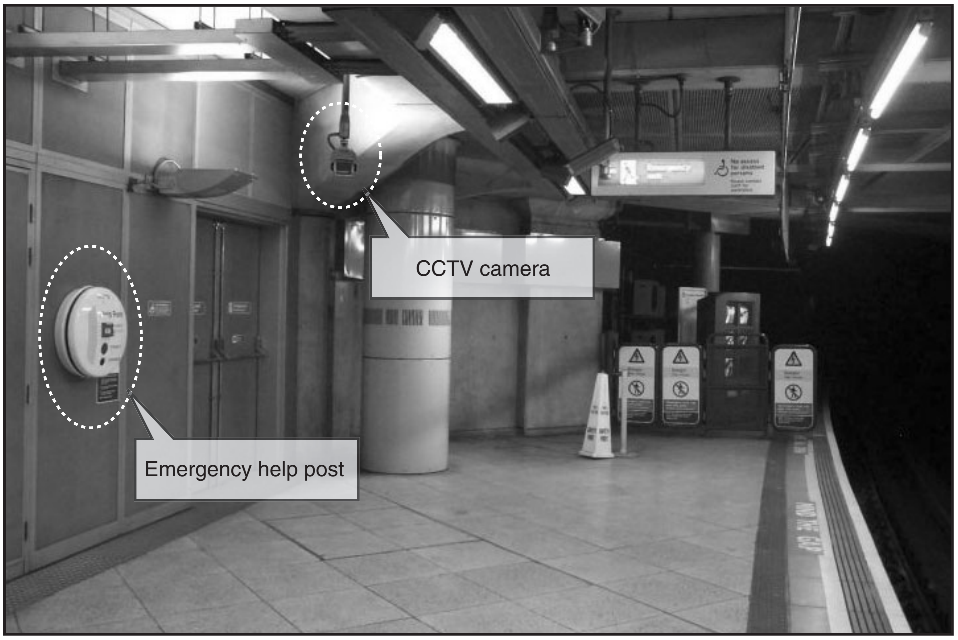


Source: London Underground.

Vending machines, as well as ticket vendors, can be designed to minimize opportunities for hiding objects above or behind them; clear plastic trash bags and clean lines of sight minimize opportunities to hide objects on the platform.

In one London station, we observed the use of netting throughout the station to help prevent objects, such as bombs, from being placed in a recessed area, such as beneath a stairwell or escalator. In this station and other stations we visited, Underground officials have installed "help posts" at which customers can call for help if an incident occurs. When these posts are activated, CCTV cameras display a video image of the help post and surrounding area to staff at a central command center. This allows the staff to directly observe the situation and respond appropriately. See figure 9 for a photograph of a help post.

Figure 9: Security Design Elements Incorporated into London's Underground



Source: London Underground.

The "help post" in this London Underground rail station allows passengers to contact station security staff in an emergency. Once activated, the CCTV camera would be turned on so security staff could monitor the situation and identify what actions to take.

Underground officials stated that the incorporation of security features in station design is an effective measure in deterring some terrorists from attacking the system. For example, officials told us that CCTV video recorded the efforts by Irish Republican Army terrorists attempting to place an explosive device inside a station—and when they could not find a suitable location to hide the device, they placed it outside in a trash can instead, thereby mitigating the impact of the explosion.

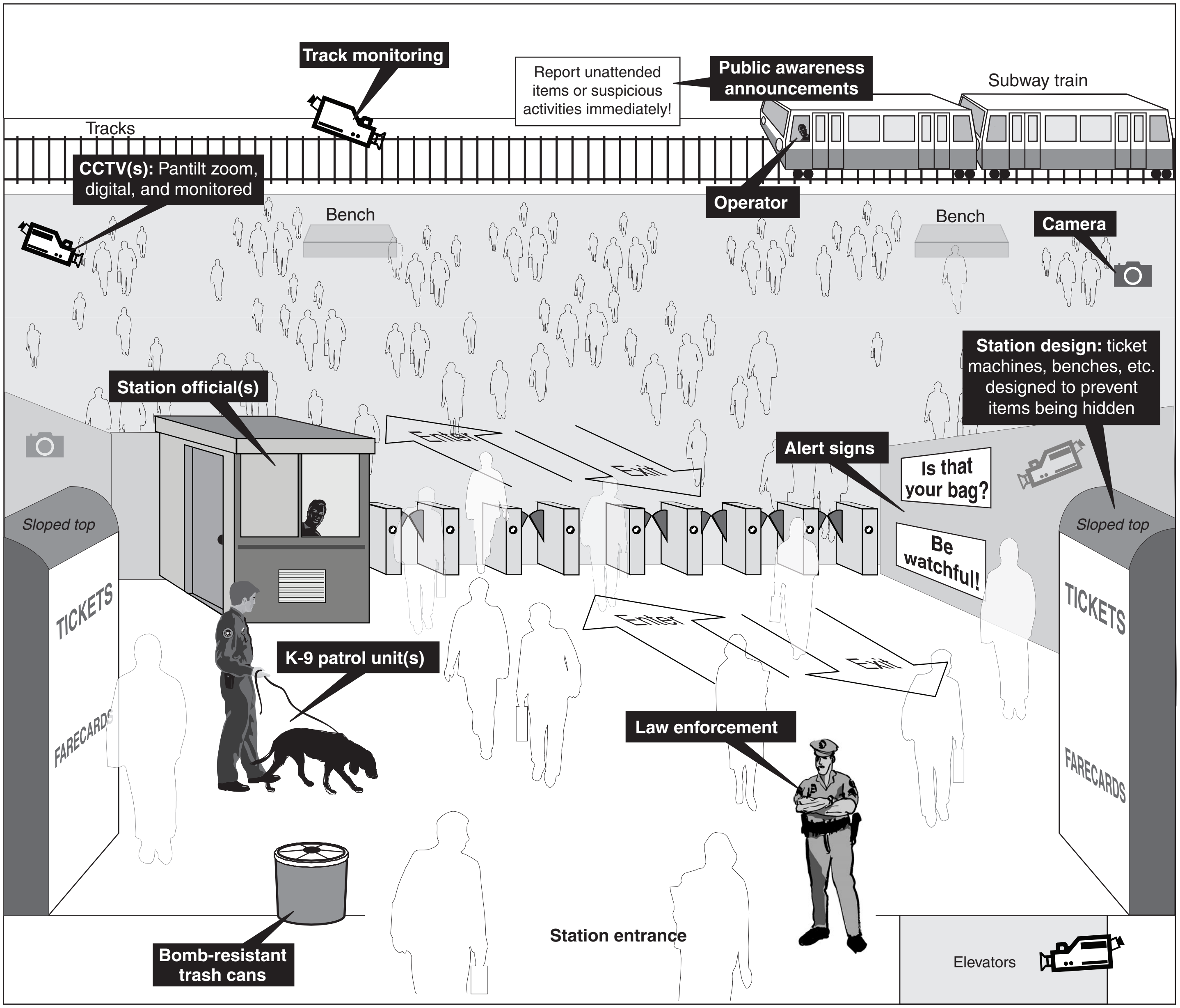
In the United States, several passenger rail operators stated that they were taking security into account when designing new facilities or remodeling older ones. Twenty-two of 32 rail operators we interviewed told us that they were incorporating security into the design of new or existing rail infrastructure. For example, New York City Transit and PATH officials told us they are incorporating security into the design of its new stations, including the redesigned Fulton Street station and the World Trade Center Hub that were damaged or destroyed during the September 11 attacks.

Under FTA's New Starts program—a discretionary grant-making program available to transit agencies seeking federal funds for new or expanded fixed-guideway system construction—a security management plan must be developed and security must be taken into consideration when designing or constructing federally funded projects. Although security-specific design considerations are required for these security plans, the plans need not incorporate a particular set of security design principles or guidelines. In June 2005, FTA issued guidelines for use by the transit industry encouraging the incorporation of particular security features into the design of transit infrastructure. These guidelines include, for example, increasing visibility for onboard staff, reducing the areas where someone could hide an explosive device on a transit vehicle, and enhancing emergency exits in transit stations. The program guidance for New Starts does not require that agencies consider these particular guidelines to further enhance station security and mitigate exposures to terrorist attack when enhancing new systems or expansions. In response to our inquiry about the feasibility and appropriateness of such a requirement, FTA officials stated that they planned to incorporate such a requirement into the program's regulations after legislation reauthorizing the New Starts program is approved.[45]

Figure 10 shows a diagram of several security measures that we observed in passenger rail stations both in the United States and abroad. It should be noted that this represents an amalgam of stations we visited, not any particular station.

[45] The New Starts program was reauthorized through the enactment of Pub. L. No. 109-59 on August 10, 2005.

Figure 10: Composite of Selected Security Practices in the Passenger Rail Environment


Track monitoring
Report unattended items or suspicious activities immediately!
Public awareness announcements
Subway train
Tracks
CCTV(s): Pantilt zoom, digital, and monitored
Operator
Bench
Bench
Camera
Station design: ticket machines, benches, etc. designed to prevent items being hidden
Station official(s)
Enter
Exit
Alert signs
Is that your bag?
Be watchful!
Sloped top
Sloped top
TICKETS
FARECARDS
TICKETS
FARECARDS
Enter
Exit
K-9 patrol unit(s)
Law enforcement
Station entrance
Bomb-resistant trash cans
Elevators

■ Security resources currently used

Source: GAO and NOVA Development Corporation.

Amtrak Faces Challenges Specific to Intercity Passenger Rail in Securing Its System

In securing its extensive system, Amtrak faces its own set of security-related challenges, some of which are different from those facing a commuter rail or transit operator. First, Amtrak operates over thousands of miles, often far from large population centers. This makes its route system much more difficult to patrol and monitor than one contained in a particular metropolitan region, and it causes delays in responding to incidents when they occur in remote areas. Also, outside the Northeast Corridor, Amtrak operates almost exclusively on tracks owned by freight rail companies. Amtrak also utilizes stations owned by freight rail companies, transit and commuter rail authorities, private corporations, and municipal governments. This means that Amtrak often cannot unilaterally make security improvements to others' rights-of-way or station facilities and that it is reliant on the staff of other organizations to patrol their facilities and respond to incidents that may occur. Furthermore, with over 500 stations, only half of which are staffed, screening even a small portion of the passengers and baggage boarding Amtrak trains is difficult. Last, Amtrak's financial condition has never been strong—Amtrak has been on the edge of bankruptcy several times—and the future of Amtrak operations is in question pending the outcome of the fiscal year 2006 budget.[46]

Amid the ongoing challenges of securing its coast-to-coast railway, Amtrak has taken some actions to enhance security throughout its intercity passenger rail system. For example, Amtrak has initiated a passenger awareness campaign, similar to those described elsewhere in this report. Also, Amtrak has begun enforcing existing restrictions on carry-on luggage that limit passengers to two carry-on bags, not exceeding 50 pounds. All bags also must have identification tags on them. Furthermore, Amtrak has begun requiring passengers to show positive identification after boarding trains when asked by staff to ensure that tickets have not been transferred or stolen, although Amtrak officials acknowledge their onboard staffs only sporadically enforce this requirement because of the numerous tasks these staff members must perform before a train departs. However, in November 2004, Amtrak implemented the Tactical Intensive Patrols (TIPS) program, under which its security staff flood selected platforms to ensure Amtrak baggage and identification requirements are met by passengers boarding

[46] The President's fiscal year 2006 budget proposed eliminating the federal government's subsidy to Amtrak. According to Amtrak officials, while the outcome of the budget is unknown at this time, severe cutbacks in Amtrak funding could reduce the amount of personnel Amtrak has available to perform security functions, while a total elimination of federal funding for Amtrak could cause a system shutdown.

trains. In addition, Amtrak increased the number of canine units patrolling its system, most of which are located in the Northeast Corridor, looking for explosives or narcotics and assigned some of its police to ride trains in the Northeast Corridor. Also, Amtrak has instituted a policy of randomly inspecting checked luggage on its trains. Finally, Amtrak is making improvements to the emergency exits in certain tunnels to make evacuating trains in the tunnels easier in the event of a crash or terrorist attack.

To ensure that security measures are applied consistently throughout Amtrak's system, Amtrak has established a series of Security Coordinating Committees, which include representatives of all Amtrak departments. These committees are to review and establish security policies, in coordination with Amtrak's police department, and have worked to develop countermeasures to specific threats. According to Amtrak, in the aftermath of the July 2005 London bombings, these committees met with Amtrak police and security staff to ensure additional security measures were implemented. Also in the wake of the London attacks, Amtrak began working with the police forces of several large east coast cities, allowing them to patrol Amtrak stations to provide extra security. In addition, all Amtrak employees now receive a "Daily Security Awareness Tip" and are receiving computer-based security training. Amtrak police officers are also now receiving specialized counterterrorism training.

While Amtrak has taken the actions outlined above, it is difficult to determine if these actions appropriately or sufficiently addressed pressing security needs. As discussed earlier, Amtrak has not performed a comprehensive terrorism risk assessment that would provide an empirical baseline for investment prioritization and decision making for Amtrak's security policies and investment plans. However, as part of the 2005 Intercity Passenger Rail Grant Program, Amtrak is required to produce a security and emergency preparedness plan, which is to include a risk assessment that Amtrak expects to finish by September 30, 2005. Upon completing this plan, Amtrak management should have a more informed basis regarding which security enhancements should receive the highest priority for implementation.

Three Foreign Rail Security Practices Are Not Currently Used in the United States

While many of the security practices we observed in foreign rail systems are similar to those U.S. passenger rail operators are implementing, we encountered three practices in other countries that were not currently in use among the domestic passenger rail operators we contacted at the time we completed our field work in June 2005, nor were they performed by the U.S. government. These practices are discussed below.

Covert testing: Two of the 13 foreign rail systems we visited utilize covert testing to keep employees alert about their security responsibilities. Covert testing involves security staff staging unannounced events to test the response of railroad staff to incidents such as suspicious packages or setting off alarms. In one European system, this covert testing involves security staff placing suspicious items throughout their system to see how long it takes operating staff to respond to the item. Similarly, one Asian rail operator's security staff will break security seals on fire extinguishers and open alarmed emergency doors randomly to see how long it takes staff to respond. Officials of these operators stated that these tests are carried out on a daily basis and are beneficial because their staff know they could be tested at any moment, and they, therefore, are more likely to be vigilant with respect to security.

Random screening: Of the 13 foreign operators we interviewed, 2 have some form of random screening of passengers and their baggage in place. In the systems where this is in place, security personnel can approach passengers either in stations or on the trains and ask them to submit their persons or their baggage to a search. Passengers declining to cooperate must leave the system. For example, in Singapore, rail agency officials rotate the stations where they conduct random searches so that the searches are carried out at a different station each day. Prior to the July 2005 London bombings, no passenger rail operators in the United States were practicing a form of random passenger or baggage screening on a continuing daily basis. However, during the Democratic National Convention in 2004, MBTA instituted a system of random screening of passengers, where every 11th passenger at certain stations and times of the day was asked to provide his or her bags to be screened. Those who refused were not allowed to ride the system. MBTA officials recognized that it is impossible to implement such a system comprehensively throughout the rail network without massive amounts of additional staff, and that even doing random screening on a regular basis would be a drain on resources. However, officials stated that such a system is workable during special events and times of heightened security but would have to be designed very carefully to ensure that passengers' civil liberties were not violated. After the July 2005 London bombings, four passenger rail operators—PATH, New York Metropolitan Transportation Authority, New Jersey Transit, and Utah Transit Authority in Salt Lake City—implemented limited forms of random bag screening in their system.[47] In addition, APTA, FTA, and the National Academy of Science's Transportation Research Board are currently conducting a study on the benefits and challenges that passenger rail operators would face in implementing a randomized passenger screening system.[48] The study is examining such issues as the legal basis for conducting passenger screening or search, the precedence for such measures in the transportation environment, the human resources required, and the financial implications and cost considerations involved. As of July 2005, an initial draft of the study was under review.

National government maintains clearinghouse on technologies and best practices: According to passenger rail operators in five countries we visited, their national governments have centralized the process for performing research and developing passenger rail security technologies and maintaining a clearinghouse on these technologies and security best practices. According to these officials, this allows rail operators to have one central source for information on the merits of a particular passenger rail security technology, such as chemical sensors, CCTVs, and intrusion detection devices. Some U.S. rail operators we interviewed expressed interest in there being a more active centralized federal research and development authority in the United States to evaluate and certify passenger rail security technologies and make that information available to rail operators. Although TSA is the primary federal agency responsible for conducting transportation security research and development, and has conducted the TRIP as previously mentioned, most of the agency's research and development efforts to date have focused on aviation security technologies. As a result, domestic rail operators told us that they rely on consultations with industry trade associations, such as APTA, to learn about best practices for passenger rail security technologies and related investments. Several rail operators stated that they were often unsure of where to turn when seeking information on security-related products, such as CCTV cameras or intrusion detection systems.

[47] According to APTA, MBTA has maintained the right to conduct random searches of passengers. In addition, after the London bombings, the Metropolitan Area Rapid Transit Authority in Atlanta posted notices on buses and trains stating that it maintains the right to conduct random searches.

[48] This research is being conducted through the Transit Cooperative Research Program, a partnership among these three entities that undertakes research and other technical activities in response to the needs of transit service providers.

Currently, many operators said they informally ask other rail operators about their experiences with a certain technology, perform their own research via the Internet or trade publications, or perform their own testing.

No federal agency has yet compiled or disseminated best practices to rail operators to aid in this process. We have previously reported that stakeholders have stated that the federal government should play a greater role in testing transportation security technology and making this information available to industry stakeholders.[49] TSA and DOT agree that making the results of research testing available to industry stakeholders could be a valuable use of federal resources by reducing the need for multiple rail operators to perform the same research and development efforts, but they have not taken action to address this.[50]

Implementing these three practices—covert testing, random screening, and a government-sponsored clearinghouse for technologies and best practices—in the United States could pose political, legal, fiscal, and cultural challenges because of the differences between the United States and these foreign nations. For instance, many foreign nations have dealt with terrorist attacks on their public transportation systems for decades, compared with the United States, where rail transportation has not been specifically targeted during terrorist attacks. According to foreign rail operators, these experiences have resulted in greater acceptance of certain security practices, such as random searches, which the U.S. public may view as a violation of their civil liberties or which may discourage them from using public transportation. The impact of security measures on passengers is an important consideration for domestic rail transit operators, since most passengers could choose another means of transportation, such as a personal automobile. As such, security measures that limit accessibility, cause delays, increase fares, or otherwise cause inconvenience could push people away from transit and into their cars. In contrast, the citizens of the European and Asian countries we visited are more dependent on public transportation than most U.S. residents and therefore, according to the rail operators we spoke with, may be more willing to accept more intrusive security measures, simply because they have no other choice for getting from place to place. Nevertheless, in order to identify innovative security measures that could help further

[49] GAO-03-843.

[50] See GAO-03-843.

mitigate terrorism-related risk to rail assets—especially as part of a broader risk management approach discussed earlier—it is important to at least consider assessing the feasibility and costs and benefits of implementing the three rail security practices we identified in foreign countries in the United States. Officials from DHS, DOT, passenger rail industry associations, and rail systems we interviewed told us that operators would benefit from such an evaluation. Furthermore, the passenger rail association officials told us that such an evaluation should include practices used by foreign rail operators that integrate security into infrastructure design.

Differences in the business models and financial status of some foreign rail operators could also affect the feasibility of adopting certain security practices in the United States. Several foreign countries we visited have privatized their passenger rail operations. Although most of the foreign rail operators we visited—even the privatized systems—rely on their governments for some type of financial assistance, two foreign rail operators generated significant revenue and profits in other business endeavors, which they said allowed them to invest heavily in security measures for their rail systems. In particular, the Paris Metro system is operated by the RATP Corporation (Regie Autonome des Transports Parisiens), which also contracts with other cities in France and throughout the world to provide consulting and project management services. RATP's ability to make a profit, according to its officials, through its consulting services allows the agency to supplement government funding in order to support expensive security measures for the Paris mass transit system. For example, RATP recently installed a computer-assisted security control system that uses CCTV, radio, and global positioning technology that it says has significantly reduced the amount of time it takes for security or emergency personnel to respond to an incident or emergency, such as a terrorist attack. Because of RATP's available funding for security, the corporation also purchased an identical system for the Metropolitan Paris Police, so the RATP and the police system would be compatible. In addition, according to Hong Kong mass transit system officials, their company was highly profitable because of its real estate and development operations, allowing the company to invest in security measures. In contrast, domestic rail operators do not generate a profit and therefore are dependent on financial assistance from the federal, state, and local levels of government to maintain and enhance services, including funding security improvements.

Another important difference between domestic and foreign rail operators is the structure of their police forces. In particular, England, France, Belgium, and Spain all have national police forces patrolling rail systems in these countries. The use of a national police force is a reflection that these foreign countries often have one nationalized rail system, rather than over 30 rail transit systems owned and operated by numerous state and local governments, as is the case in the United States. For example, in France, the French National Railway operates all intercity passenger rail services in the country and utilizes the French Railway police to provide security. According to foreign rail operators, the use of one national rail police force allows for consistent policing and security measures throughout the country. In the United States, in contrast, there is not a national police force for the rail transit systems.[51] Rather, some transit agencies maintain individual polices forces, while others rely on their city or county police forces for security.

Conclusions

The recent London rail bombings made clear that even when a variety of security precautions are put in place, passenger rail systems that move high volumes of passengers on a daily basis remain vulnerable to attack. It is important nonetheless to take the necessary steps to identify and mitigate risks to passenger rail systems. In the United States, securing the passenger rail system is a daunting task. As we have reported previously, the sheer number of stakeholders involved in securing these systems can lead to communication challenges, duplication of effort, and confusion about roles and responsibilities. Accordingly, enhanced federal leadership is needed to help ensure that actions and investments designed to enhance security are properly focused and prioritized. We are encouraged by the steps DHS components have taken to use elements of a risk management approach to guide critical infrastructure protection decisions for the passenger rail industry. This is a necessary step in a broader effort by DHS to determine how to allocate finite resources not only to help protect all modes of transportation, but also to secure other national critical infrastructure sectors.

However, both DHS and TSA could take additional steps to help ensure that the risk management efforts under way clearly and effectively identify priority areas for security-related investments in rail and other sectors. We recognize that TSA has had many aviation security-related responsibilities and has implemented many security initiatives to meet legislative

[51] Unlike domestic rail transit agencies, Amtrak maintains a 342-member police force for its national network.

requirements. Notwithstanding, TSA has not yet completed its methodology for determining how the results of threat, criticality, and vulnerability assessments will be used to identify and prioritize risks to passenger rail and other transportation sectors. In order to complete and apply its methodology as part of the forthcoming transportation sector-specific plan, TSA needs to more consistently involve industry stakeholders in the overall risk assessment process and collaborate with them on collecting and analyzing information on critical infrastructure and key resources in the passenger rail industry. Without consistent and substantive stakeholder input, TSA may not be able to fully capture critical information on rail assets—information that is needed to properly assess risk. In addition, as part of the process to complete its risk assessment methodology, TSA needs to consider whether other proven approaches, such as ODP's risk assessment methodology, could be leveraged for rail and other transportation modes, such as aviation. Until the overall risk to the entire transportation sector is identified, TSA will not be able to fully benefit from the outcome of risk management analysis—including determining where and how to target the nation's limited resources to achieve the greatest security gains.

Once risk assessments for the passenger rail industry have been completed, it will be critical to be able to compare assessment results across all transportation modes as well as other critical sectors and make informed, risk-based investment trade-offs. The framework that DHS is developing to help ensure that risks to all sectors can be analyzed and compared in a consistent way needs to be completed and shared with TSA and other sector-specific agencies. The delay in completing the element of the framework that defines concepts, terminology, and metrics for assessing risk limits DHS's ability to compare risk across sectors as sector-specific agencies are concurrently conducting risk assessment activities without this guidance. Until this framework is complete, it will not be possible for information from different sectors to be reconciled to allow for a meaningful comparison of risk—a goal outlined in DHS's interim NIPP.

Apart from its efforts to formally identify risks, TSA has taken steps to enhance the security of the overall passenger rail system. The issuance of security directives in the wake of the Madrid bombings was a well-intentioned effort to take swift action in response to a current threat. However, because these directives were issued under emergency circumstances, with limited input and review by rail industry and federal stakeholders—and no public comment period—they may not provide the industry with baseline security standards based on industry best practices.

Nor is it clear how these directives are to be measured and enforced. Consequently, neither the federal government nor rail operators can be sure they are requiring and implementing security practices proven to help prevent or mitigate disasters. Collaborating with rail industry stakeholders to develop security standards is an important starting point for strengthening the security of passenger rail systems. DHS and DOT have taken steps in this direction through the interdepartmental MOU in place and related agreements now being developed to define roles and responsibilities and resources for mass transit, rail, and other matters. These agreements, once completed and communicated to the rail industry, will help ensure that federal activities to secure rail systems, including the development of standards, are coordinated, and that stakeholders are involved in their development and implementation to the extent possible. Otherwise, security efforts could be duplicative, thus dispersing finite resources, rather than focusing them based on risk, or fail to achieve the intended ends. Given the importance of clearly defining DHS's and DOT's roles and responsibilities for rail security matters, time frames could be established to hold DHS and DOT accountable for completing the MOU agreements.

While foreign passenger rail operators face similar challenges to securing their systems and have generally implemented similar security practices as U.S. rail operators, there are some practices that are utilized abroad that U.S. rail operators or the federal government have not studied in terms of the feasibility, costs, and benefits. For example, an information clearinghouse for new passenger rail technologies that are available and have been tested might allow rail operators to efficiently implement technologies that had already received approval. In addition, while FTA plans to require rail operators to consider its security infrastructure design guidelines when renovating or constructing rail systems or facilities, opportunities may still exist to further research and evaluate ways of integrating security into design, as some foreign rail operators have done. Another rail security practice—covert testing of rail security procedures—is being used in two foreign rail systems we visited and is considered by them as an effective means of keeping rail employees alert to their surroundings and potential security threats. And finally, random searches of passengers and baggage are being used by two foreign rail operators and this practice has recently been adopted by four domestic rail operators in the wake of the London attacks.

Introducing these security practices into the United States may involve cultural, financial, and political challenges, owing to differences between the United States and foreign nations. Nonetheless, as part of the overall risk management approach, there may be compelling reasons for exploring the feasibility, costs, and benefits of implementing any of these practices in the United States. Doing so could enable the United States to leverage the experiences and knowledge of foreign passenger rail operators and help identify additional innovative measures to secure rail systems against terrorist attack in this country.

Recommendations for Executive Action

In order for the Department of Homeland Security to have the information needed to fully evaluate, compare, and prioritize risk mitigation activities across sectors, we recommend that the Secretary of the Department of Homeland Security take the following action:

- Establish a timeline for completing the department's framework for analyzing sector risks and ensure that the risk assessment methodologies used by sector-specific agencies are consistent with this framework.

In order for the Transportation Security Administration to have the information needed to more fully evaluate, select, and implement risk mitigation activities, and complete its transportation sector-specific plan and other strategic risk based plans, we recommend that the Secretary of the Department of Homeland Security direct the Assistant Secretary of the Transportation Security Administration to take the following two actions:

- Establish a plan for completing its methodology for conducting risk assessments that includes timelines and addresses how it will work with passenger rail stakeholders and leverage existing federal expertise in Department of Homeland Security components, including the Office for Domestic Preparedness, as well as the Department of Transportation modal administrations, including the Federal Railroad Administration and the Federal Transit Administration.

- Evaluate whether the risk assessment methodology used by the Office for Domestic Preparedness should be leveraged to facilitate the completion of risk assessments for rail and other transportation modes.

To ensure that future rail security directives are enforceable, transparent, and feasible, we recommend that the Secretary of the Department of Homeland Security direct the Assistant Secretary of the Transportation Security Administration, in collaboration with the Department of Transportation and the passenger rail industry, to take the following two actions:

- Develop security standards that reflect industry best practices and can be measured, monitored, and enforced by Transportation Security Administration rail inspectors and, if appropriate, by rail asset owners. This could be accomplished by using the rule-making process, with notice in the Federal Register and an opportunity for interested stakeholders to comment, to promulgate long-term regulations that incorporate these standards.

- Set timelines for completing the memorandum of understanding modal agreements for rail, mass transit, and research and development, which both the Department of Homeland Security and the Department of Transportation have agreed to pursue.

To help strengthen the security of passenger rail systems in the United States and potentially leverage the knowledge and practices employed by foreign rail operators, we recommend that the Secretary of the Department of Homeland Security, in collaboration with the Department of Transportation and the passenger rail industry, take the following two actions:

- Evaluate the feasibility of establishing and maintaining an information clearinghouse on existing and emergency security technologies and security best practices used in the passenger rail industry both in the United States and abroad.

- Evaluate the potential benefits and applicability—as risk analyses warrant and as opportunities permit—of implementing covert testing processes to evaluate the effectiveness of rail system security personnel; implementing practices used by foreign rail operators that integrate security into infrastructure design; and implementing random searches or screening of passengers and their baggage, pending the results of an ongoing joint federal and industry review of the impact of random screening on passenger rail operators.

Agency Comments and Our Evaluation

We provided DHS, DOT, and Amtrak a draft of this report for review and comment. DOT and Amtrak generally agreed with our findings and recommendations and provided technical comments, which we incorporated where appropriate.

DHS generally concurred with the report's recommendations and provided detailed comments on various sections of the report. Its comments are contained in appendix IV. We summarize their comments and provide our response below.

In commenting on the report, DHS stated that it is working through the Office of State and Local Government Coordination Preparedness (referred to in this report as the Office for Domestic Preparedness, ODP), TSA, and FTA to maximize and leverage collective resources to better serve the mass transit and commuter rail industry. In addition, DHS indicated that it will share ODP's risk management architecture with public and private sector entities and use risk management principles to better prioritize its funding decisions. DHS reported taking or is planning to take other actions to enhance the security of the U.S. passenger rail system, such as initiating a canine explosives detection program, gathering and centralizing information on mass transit security to aid in decision making, and partnering with FRA inspectors to review rail security measures in operation since the July 2005 London rail bombings. We are encouraged by DHS's efforts to work towards a common risk-based architecture for securing the passenger rail system and its related security initiatives.

In more specific comments, DHS stated that our assertion that TSA missed the December 2004 deadline for completing the TSSP was misleading because the agency completed a draft by November 2004. DHS also stated that it plans to include industry associations, such as APTA and AAR, in its development of the TSSP and noted that it partnered with these associations and their members after the London bombings in July 2005. We modified the report to reflect the fact that a draft TSSP was completed by this date. However, the plan was not produced by December 2004, as required by HSPD-7, and therefore was not available for use by the rail operators and stakeholders.

DHS also noted that while TSA's methodology for conducting criticality assessments relies on open source information and therefore does not require direct contact with industry stakeholders, the agency nevertheless involved federal stakeholders and rail operators in conducting the assessments. We recognize that TSA's process for conducting criticality assessments relies on open source information, and TSA reported to us that it had some contact with stakeholders. However, DHS's interim NIPP states that the department and sector-specific agencies would work with the industry to determine the most effective means of collecting and analyzing information on critical assets. TSA was not able to provide us with evidence showing that it had solicited and evaluated input from industry stakeholders on its criticality assessment methodology. In addition, the criticality assessment case files we reviewed contained no evidence of coordination with stakeholders during the assessment process. Furthermore, industry associations we interviewed told us that

TSA did not solicit their input on the agency's criticality assessment methodology or ask them to identify specific critical assets. Moreover, of the 32 rail operators we contacted about TSA's criticality assessment process, 22 operators responded; of those who responded, all stated that TSA did not involve them in conducting critical assessments of their systems.

DHS also stated that while stakeholders were not given an opportunity to comment on the final draft of the measures contained in the security directives, various stakeholders, including Amtrak, did comment on each of the measures required by the directive. Our report acknowledges that associations and Amtrak were given an opportunity to comment on the draft directives. However, the draft directives initially provided to industry stakeholders did not include all of the measures required by the final directives. For example, the draft directives provided to APTA and AAR did not include the requirement that engineer cab or compartments be kept locked. Moreover, although TSA stated that it would continue to collaborate with industry stakeholders on the development of the directives, DHS and TSA determined that the prevailing threat environment necessitated issuing the directives without additional consultation. According to TSA, the emergency circumstances under which the directives were issued allowed for only limited input and review by federal and rail industry stakeholders. However, we believe that using the federal rule-making process as a means of establishing permanent standards would make the process more transparent and could help TSA in developing standards that are most appropriate for the industry and which can be measured, monitored, and enforced. Since stakeholders will play a critical role in administering, implementing, and/or enforcing TSA standards, their involvement in the development of standards is important to the success of these initiatives.

DHS stated that our report criticized TSA's efforts to develop the directives based upon consultation with industry and a review of best security practices. Specifically, DHS said that TSA went beyond FTA's and APTA's written documents (i.e., FTA's list of the top 20 actions FTA rail operators can take to strengthen security, FTA-recommended protective measures and activities for transit agencies that may be followed based on current threat levels, and an APTA member survey) and considered other effective security measures, such as locking engineer cab and compartment doors (a measure suggested by WMATA, according to DHS), which the agency said were being implemented by various operators. While we agree that collaborating with other federal agencies and industry stakeholders to develop security standards based upon best practices is a critical step in enhancing the security of U.S. passenger rail systems and are making a recommendation to this effect, we continue to question the extent to which TSA followed this approach in developing the directives and the criteria TSA used to determine what constituted industry best practices. For example, regarding the requirement to lock train operator cabs or compartments, it is unclear whether this requirement is an industry best practice. The source material TSA provided to us, which the agency said it consulted in developing the directives, does not indicate that locking engineer or train operator cab or compartment doors is a best practice, or an effective one, in use by WMATA or other operators. Furthermore, TSA did not seek input from other stakeholders to determine whether they viewed this as a best practice. For example, the draft directives provided to AAR and APTA for comment did not include this measure. In addition, documentation shows that TSA called one commuter rail operator prior to issuing the directives to discuss this proposed measure, and the operator raised a concern about the safety of the locked door requirement. All of the rail operators and association representatives we interviewed raised concerns either about the extent of TSA's coordination with the industry in developing the directives or the feasibility of specific directives.

Regarding our assertion that the locked door measure may conflict with an FRA safety requirement, DHS responded that, according to FRA, the measure applied only to two types of passenger rail cars. However, FRA's director of the office of safety assurance and compliance and its director of security disagreed with this assertion and said that this safety concern would apply to all commuter or intercity rail equipment that is equipped with locking mechanisms. While the locked door requirement may be well intentioned, it may have the unintended consequence of increasing safety risks to railroad employees and passengers. According to FRA, a locked door pursuant to the directive would not allow the locomotive engineer to quickly exit the cab when faced with an impending highway rail grade crossing collision or other accident. In some cases, the door providing access to the locomotive's cab also serves as one of only two primary paths for emergency exit by passengers and is marked as an emergency exit. According to FRA, if these doors are locked pursuant to the directives, they may not be usable in an emergency, and passenger evacuation time could be substantially increased.

In the report, we stated that APTA, AAR, and other stakeholders did not believe they had been sufficiently consulted throughout the development of the security directives, including the measure advocating installation of bomb-resistant trash cans. As a result, stakeholders did not believe the directives reflected a complete understanding of the passenger rail environment or incorporate industry best practices. On this issue, DHS noted in its comments that the directives did not require the installation of bomb-resistant trash cans, but rather encouraged the removal of traditional trash cans. While we agree that the directive emphasizes the desirability, under certain circumstances and to the extent that resources allow, of removing traditional trash cans, we believe the directive also directly advocates the use of bomb-resistant trash cans since it directs operators to "install bomb resistant receptacles to the extent resources allow." While industry stakeholders had an opportunity to comment on the trash can removal issue, they were not given an opportunity to consider the feasibility or efficacy of installing bomb-resistant trash cans because this measure was not included in the draft directives provided to industry stakeholders for comment.

With regard to the directive requiring Amtrak and the Alaska Railroad Corporation to perform ID checks on all passengers, DHS stated that our report raised an issue regarding the efficacy of performing ID checks without vetting passenger names against a watch list or other database. DHS stated that ID checks were a baseline measure that could be enhanced in response to heightened or specific threats by vetting names against a watch list. DHS also explained that Amtrak was already performing some ID checks, and that the measure was designed to incorporate the ID check into current business practice of operators such as Amtrak, which could request passengers to have their IDs available when tickets are checked. We do not disagree with DHS's assertion that additional measures could be added in heightened threat environments. Our discussion of this measure focuses on Amtrak's concern about the feasibility of the requirement in light of the potential impacts on Amtrak's operations and revenue. DHS's explanation of the intent of this measure suggests that it was to encourage the use of ID checks and that operators "could request passengers to have their ID available." However, as written, the directive requires rather than encourages IDs to be checked at the initial point where tickets are checked.

In commenting on our report's assertion that it is unclear which entities are responsible for implementing the security directives, DHS acknowledged that individual stations and terminals may be owned and/or operated by multiple federal, state, and private entities but emphasized that the prevailing threat environment at the time the security directives were issued necessitated looking to the passenger rail operator to coordinate the implementation of the required measures. We agree that rail operators must play an important role in the implementation of measures in stations that they may not own. However, the directives, as written, do not make it clear which entities (rail operators and station and terminal owners) are responsible for implementing the requirements and, in the 15 months since the directives were issued, TSA has not yet clarified these responsibilities. The industry associations and rail operators still believe that implementation responsibilities remain unclear. Given that TSA considers these directives to be mandatory and has hired inspectors to ensure compliance with directives, we believe that it is important to clearly articulate which entities are to be held accountable for implementing the measures required by the directives.

Finally, DHS commented that it has approved and distributed standard operating procedures to its rail inspectors since we completed our field work, and that DOT had been actively engaged in reviewing and commenting on these procedures. We are encouraged that TSA is moving forward with efforts to develop processes for ensuring compliance with security standards. However, as stated above, we are concerned that TSA may not be effectively able to ensure or enforce compliance until the standards have been more fully developed in consultation with stakeholders. TSA was not able to provide us with evidence to show it had collaborated with DOT in developing and approving these procedures. In addition, DOT officials raised questions regarding the approved status of these procedures. For example, FTA's director of safety and security told us he had not seen either a draft or a final version of these procedures. Furthermore, FRA's director of the office of safety assurance and compliance did not believe the procedures had been approved. According this official, TSA provided a draft of the standard operating procedures on August 10, 2005, and comments are due back on September 14, 2005.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution of it until 30 days from the date of this letter. We will then send copies of this report to the Secretary of Homeland Security, the Secretary of Transportation, the Assistant Secretary of the Transportation Security Administration, the Administrator of the Federal Railroad Administration, the Administrator of the Federal Transit Administration, the President and Chief Executive Officer of Amtrak, the Director of the Office of State and Local Government Coordination and Preparedness, and interested congressional committees. We will make copies available to others upon request. In addition, this report will be available at no charge on our Web site at http://www.gao.gov.

If you or your staff have any questions about this report, please contact Ms. Cathleen Berrick on (202) 512-8777 or Ms. JayEtta Hecker on (202) 512-2834. Contact points for our offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix V.

Cathleen A. Berrick

Cathleen A. Berrick, Director
Homeland Security and Justice Issues

JayEtta Hecker

JayEtta Hecker, Director
Physical Infrastructure Issues

Appendix I: Objectives, Scope, and Methodology

To address our first objective, to identify the actions taken by the Department of Homeland Security (DHS) agencies to assess risks posed by terrorism in the context of prevailing risk management principles, we interviewed officials from DHS, the Department of Transportation (DOT), and Amtrak. Specifically, within DHS, we interviewed officials from the Transportation Security Administration's (TSA) Office of Intermodal Security Programs (formerly the Office of Maritime and Land Security), Office of Transportation Security Policy, Transportation Security Intelligence Service, and the Chief Operating Officer. We also interviewed officials from the Office of State and Local Government Coordination and Preparedness (SLGCP), the Information Analysis and Infrastructure Protection Directorate, the Border and Transportation Security Directorate, and the Office of Inspector General. Within DOT, we interviewed officials from the Office of Intelligence, Inspector General, Deputy Secretary of Transportation, the Federal Transit Administrations (FTA) Office of Safety and Security, and the Federal Railroad Administration (FRA) Office of Security and Office of Safety Assurance and Compliance. We also interviewed Amtrak's Chief of Police and Security, Vice President of Corporate Security, Inspector General, and Amtrak security officials in locations throughout the United States. In addition, we reviewed federal agency plans such as the DHS Interim National Infrastructure Protection Plan, and obtained and reviewed various risk-related assessments conducted by federal agencies, including the vulnerability assessments of rail transit systems conducted by FTA, TSA threat assessments of mass transit and rail and criticality assessments of passenger rail assets, and a passenger rail risk assessment tool kit developed by SLGCP. Further, we conducted a site visit to and interview with officials from the Port Authority of New York and New Jersey to discuss the results of an SLGCP risk assessment conducted at that location.

To address our second objective to determine the actions that federal agencies have taken to enhance the security of the U.S. passenger rail system, we interviewed officials from FTA's Office of Safety and Security, DOT's Office of the Secretary, FRA's Office of Security, Office of Research and Development, and Office of Safety Assurance and Compliance, and TSA's Office of Intermodal Security Programs, Office of Research and Development, and the Chief Operating Officer. We did not evaluate the effectiveness of any of these federal passenger rail security efforts. We also reviewed federal guidance, such as Homeland Security Presidential Directive-7, FTA's Top 20 Security Program Action Items for Transit Agencies, and TSA's security directives for passenger rail operators;

inspected all phases of TSA's TRIP program; and reviewed the memorandum of understanding between DHS and DOT.

To determine the security practices that domestic and selected foreign passenger rail operators have implemented to mitigate risks and enhance security, and any differences in these practices, we interviewed officials from TSA's Office of Intermodal Security Programs, FRA's Office of International Policy, and FTA's Office of Safety and Security to discuss domestic and foreign passenger rail security measures. We also conducted site visits to or teleconferences with 32 heavy and commuter rail operators in the United States—representing over 95 percent of the nation's passenger rail ridership in 2003—and Amtrak. Table 4 lists the domestic passenger rail operators that we visited or interviewed during our review.

Table 4: Domestic Passenger Rail Agencies We Visited or Interviewed for the Purposes of this Review

Passenger rail agency	Urban area served
Altamont Commuter Express (ACE)	Stockton and San Jose, California
Alaska Railroad Corporation	Anchorage and Fairbanks, Alaska
Bay Area Rapid Transit (BART)	San Francisco–Oakland, California
CALTRAIN	San Francisco and San Jose, California
San Diego Transit Corp. (Coaster)	San Diego, California
Dallas Area Rapid Transit / Trinity Railway Express (DART)	Dallas, Texas
Greater Cleveland Regional Transportation Authority (GCRTA)	Cleveland, Ohio
Los Angeles County Metropolitan Transportation Authority (LACMTA)	Los Angeles, California
Metropolitan Atlanta Rapid Transit Authority (MARTA)	Atlanta, Georgia
Maryland Transit Administration (MTA)	Greater Washington, D.C., and Maryland
Massachusetts Bay Transportation Authority (MBTA)	Boston, Massachusetts
METRA Commuter Rail	Chicago, Illinois
Southern California Regional Rail Authority (Metrolink)	Greater Los Angeles, California
Long Island Railroad (LIRR)	New York, New York
Metro North Railroad (MNR)	New York, New York
New York City Transit (NYCT)	New York, New York

Passenger rail agency	Urban area served
Staten Island Railway (SIR)	New York, New York
San Francisco Municipal Railway (MUNI)	San Francisco, California
Northern Indiana Commuter District	Chicago, Illinois–-Northern Indiana
Delaware River Port Authority (PATCO)	New Jersey and Philadelphia, Pennsylvania
Port Authority Trans Hudson (PATH)	New York, New York–-New Jersey
San Diego Trolley	San Diego, California
Southeastern Pennsylvania Transportation Authority (SEPTA)	Philadelphia, Pennsylvania
South Florida Regional Transportation Authority (SFRTA)	Miami, Florida
Connecticut Department of Transportation (Shore Line East)	New Haven, Connecticut
Sound Transit (Sounder)	Seattle, Washington
TRIMET	Portland, Oregon
Virginia Railway Express (VRE)	Northern Virginia, Greater Washington, D.C.
Washington Metropolitan Area Transit Authority (WMATA)	Washington, D.C.
New Jersey Transit (NJT)	Newark, New Jersey– New York, New York
Miami Dade Transit	Miami, Florida
Chicago Transit Authority (CTA)	Chicago, Illinois

Source: National Transit Database.

We also conducted site visits to 13 passenger rail operators in seven European and Asian countries, including France, the United Kingdom, Belgium, Spain, Japan, Singapore, and Hong Kong. In all of these countries, we met with passenger rail security officials and toured facilities to identify security practices being used on their systems as well as differences from U.S. passenger rail systems. We also met with government officials in select countries. See table 5 for a list of foreign passenger rail operators and government agencies we met with abroad.

Table 5: Foreign Passenger Rail and Government Agencies We Visited or Interviewed for the Purposes of This Review

Passenger rail agency or government agency	Area served
Paris Metro	Paris, France
French National Railway	France
National Department for Transport—Security Directorate	United Kingdom
London Underground	London, United Kingdom
Network Rail	United Kingdom
British Transport Police	United Kingdom
Channel Tunnel Rail Link	United Kingdom/France
Transport for London	London, United Kingdom
Belgian National Railway	Belgium
Madrid Metro	Madrid, Spain
RENFE (Spanish National Railway)	Spain
European Commission—Directorate for Energy and Transport	European Union
JR Central	Japan
Tokyo Metro	Tokyo, Japan
Ministry of Land, Infrastructure, and Transport	Japan
SBS Transit Corporation	Singapore
Singapore Mass Rapid Transit	Singapore
Land Transport Authority	Singapore
Hong Kong Mass Transit Railway	Hong Kong
Special Administrative Regional Government	Hong Kong

Source: GAO.

We also attended an international rail security conference sponsored by the International Union of Railways in partnership with the International Union on Public Transport. While attending this conference, we interviewed officials from the German National Railway. Because we selected a nonprobability sample of both foreign and domestic passenger rail operators, the information we obtained from these interviews and visits cannot be generalized to all foreign or domestic rail operators. Finally, we discussed those foreign security practices identified with several domestic passenger rail operators and a collection of surface transportation security experts from the Mineta Transportation Institute and RAND Corporation to determine the potential to use some of these practices in the United States.

We performed our work from May 2004 through July 2005 in accordance with generally accepted government auditing standards.

Appendix II: Elements of a Typical Homeland Security Risk Assessment

A threat assessment: Threat is defined as a potential intent to cause harm or damage to an asset (e.g., natural environment, people, man-made infrastructures, and activities and operations). Threat assessments consist of the identification of adverse events that can potentially affect an entity. Threats might be present at the global, national, or local level, and their sources include terrorists and criminal enterprises. Specific threat information may indicate vulnerabilities that are subject to attack, or following the completion of a risk management process may, for instance, indicate that resources should be temporarily deployed to protect cargo in a particular region of the country or a specific airport. Even if updated often, a threat assessment might not adequately capture some emerging threats.

A vulnerability assessment: Vulnerability is defined as the inherent state (either physical, technical, or operational) of an asset that can be exploited by an adversary to cause harm or damage. Vulnerability assessments identify these inherent states and the extent of their susceptibility to exploitation, relative to the existence of any countermeasures. A vulnerability assessment is generally conducted by a team of experts skilled in such areas as engineering, intelligence, security, information systems, finance, and other disciplines.

A criticality assessment: Criticality is defined as an asset's relative importance, given that an event occurs. Criticality or similar consequence assessments identify and evaluate an entity's assets based on a variety of factors, including the importance of its mission or function, the extent to which people are at risk, or the significance of a structure or system in terms of, for example, national security, economic activity, or public safety. Criticality or consequence assessments are important because they provide, in combination with threat and vulnerability assessments, information for later stages of the risk management process.

Risk assessment: A complete risk assessment is a qualitative and/or quantitative determination of the likelihood (probability) of occurrence of an adverse event and the severity, or impact, of its consequences. Risk assessment can involve designating risk as, for example, low, medium, or high (other scales, such as numeric, can also be used), and often integrates threat, criticality, and vulnerability assessments. Such analyses can help inform which actions are best suited to mitigate assessed risk, in conjunction with the risk-based evaluation of alternatives while considering cost and other factors.

Source: GAO.

Appendix III: FTA and ODP Passenger Rail Risk Assessments Conducted or In Progress

FTA Risk Assessments Conducted

1. Bi-State Development Agency
2. Chicago Metra Commuter Rail
3. Chicago Transit Authority
4. Dallas Areas Rapid Transit–Trinity Railway Express
5. Denver Regional Transportation District
6. Detroit Department of Transportation
7. Greater Cleveland Regional Transit Authority
8. King County Department of Transportation Metro District
9. Los Angeles County Metropolitan Transportation Authority
10. Maryland Transit Administration
11. Massachusetts Bay Transportation Authority
12. Metropolitan Transit Authority of Harris County
13. Metropolitan Atlanta Rapid Transit Authority
14. Metropolitan Transportation Authority--Long Island Railroad
15. Metropolitan Transportation Authority--Metro North Railroad
16. Metropolitan Transportation Authority--New York City Transit
17. Miami Dade Transit
18. Minneapolis Metro Transit
19. New Jersey Transit
20. New Orleans Regional Transit Authority
21. Niagara Frontier Transportation Authority
22. North County Transit District–Coaster
23. Port Authority Trans-Hudson–PATH

24. Port Authority of Allegheny County Pennsylvania
25. Puerto Rico Highway and Transportation Authority
26. Sacramento Regional Transit District
27. San Diego Trolley
28. Santa Clara Valley Transit Authority
29. San Francisco Municipal Railway–MUNI
30. San Francisco Bay Area Rapid Transit
31. Southeastern Pennsylvania Transportation Authority
32. Tri-County Commuter Rail Authority
33. Tri-County Metropolitan Transportation District of Oregon–TriMet
34. Utah Transit Authority
35. Virginia Railway Express
36. Washington Metropolitan Area Transit Authority

ODP Risk Assessments

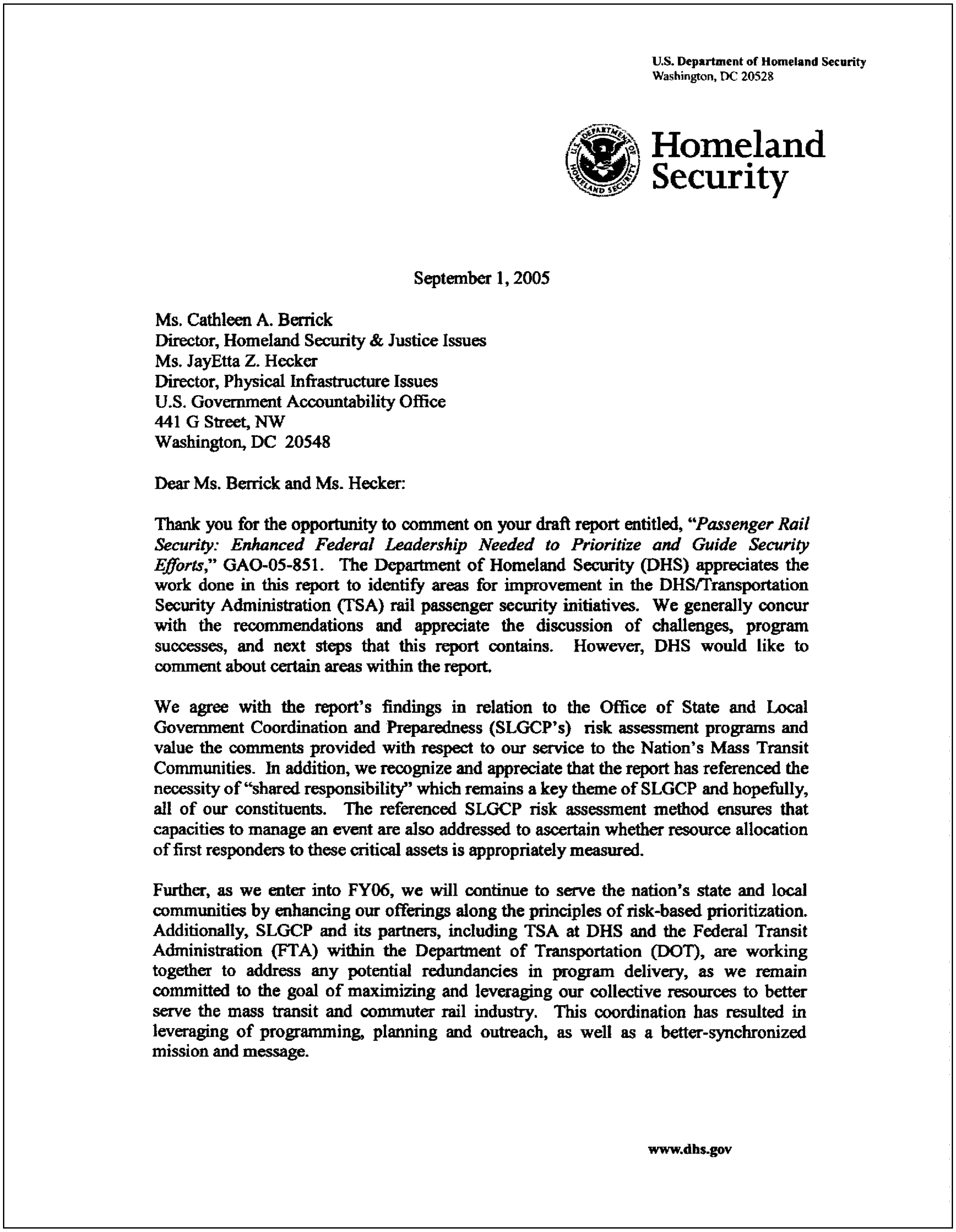
Completed

1. Port Authority of New York and New Jersey
2. New Jersey Transit
3. Massachusetts Bay Transportation Authority
4. Washington Metropolitan Area Transit Authority
5. Southeastern Pennsylvania Transportation Authority
6. Tri-County Metropolitan Transportation District of Oregon–TriMet
7. Delaware River Port Authority—PATCO

In Progress

1. Bay Area Rapid Transit
2. San Mateo County Transit District
3. San Francisco Municipal Railway
4. Metropolitan Transit Authority of Harris County, Texas
5. Chicago Transit Authority
6. Miami-Dade Transit
7. Metropolitan Atlanta Rapid Transit Authority
8. AMTRAK Northeast Corridor
9. Dallas Area Rapid Transit / Trinity Railway Express
10. South Florida Regional Transportation Authority
11. Maryland Transit Administration
12. Detroit Transportation Corporation

Appendix IV: Comments from the Department of Homeland Security



U.S. Department of Homeland Security
Washington, DC 20528

Homeland
Security

September 1, 2005

Ms. Cathleen A. Berrick
Director, Homeland Security & Justice Issues
Ms. JayEtta Z. Hecker
Director, Physical Infrastructure Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

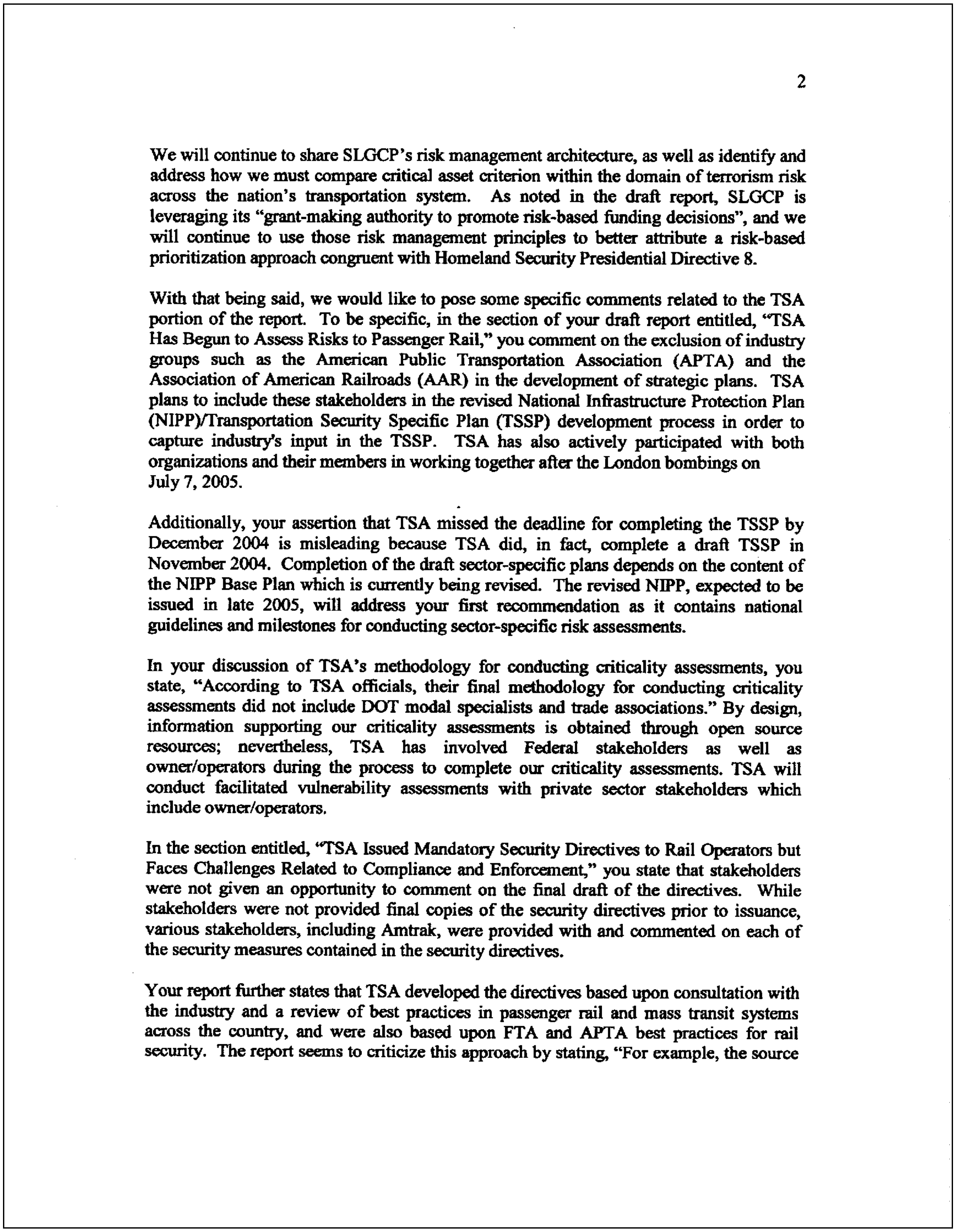
Dear Ms. Berrick and Ms. Hecker:

Thank you for the opportunity to comment on your draft report entitled, "*Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts*," GAO-05-851. The Department of Homeland Security (DHS) appreciates the work done in this report to identify areas for improvement in the DHS/Transportation Security Administration (TSA) rail passenger security initiatives. We generally concur with the recommendations and appreciate the discussion of challenges, program successes, and next steps that this report contains. However, DHS would like to comment about certain areas within the report.

We agree with the report's findings in relation to the Office of State and Local Government Coordination and Preparedness (SLGCP's) risk assessment programs and value the comments provided with respect to our service to the Nation's Mass Transit Communities. In addition, we recognize and appreciate that the report has referenced the necessity of "shared responsibility" which remains a key theme of SLGCP and hopefully, all of our constituents. The referenced SLGCP risk assessment method ensures that capacities to manage an event are also addressed to ascertain whether resource allocation of first responders to these critical assets is appropriately measured.

Further, as we enter into FY06, we will continue to serve the nation's state and local communities by enhancing our offerings along the principles of risk-based prioritization. Additionally, SLGCP and its partners, including TSA at DHS and the Federal Transit Administration (FTA) within the Department of Transportation (DOT), are working together to address any potential redundancies in program delivery, as we remain committed to the goal of maximizing and leveraging our collective resources to better serve the mass transit and commuter rail industry. This coordination has resulted in leveraging of programming, planning and outreach, as well as a better-synchronized mission and message.

www.dhs.gov



We will continue to share SLGCP's risk management architecture, as well as identify and address how we must compare critical asset criterion within the domain of terrorism risk across the nation's transportation system. As noted in the draft report, SLGCP is leveraging its "grant-making authority to promote risk-based funding decisions", and we will continue to use those risk management principles to better attribute a risk-based prioritization approach congruent with Homeland Security Presidential Directive 8.

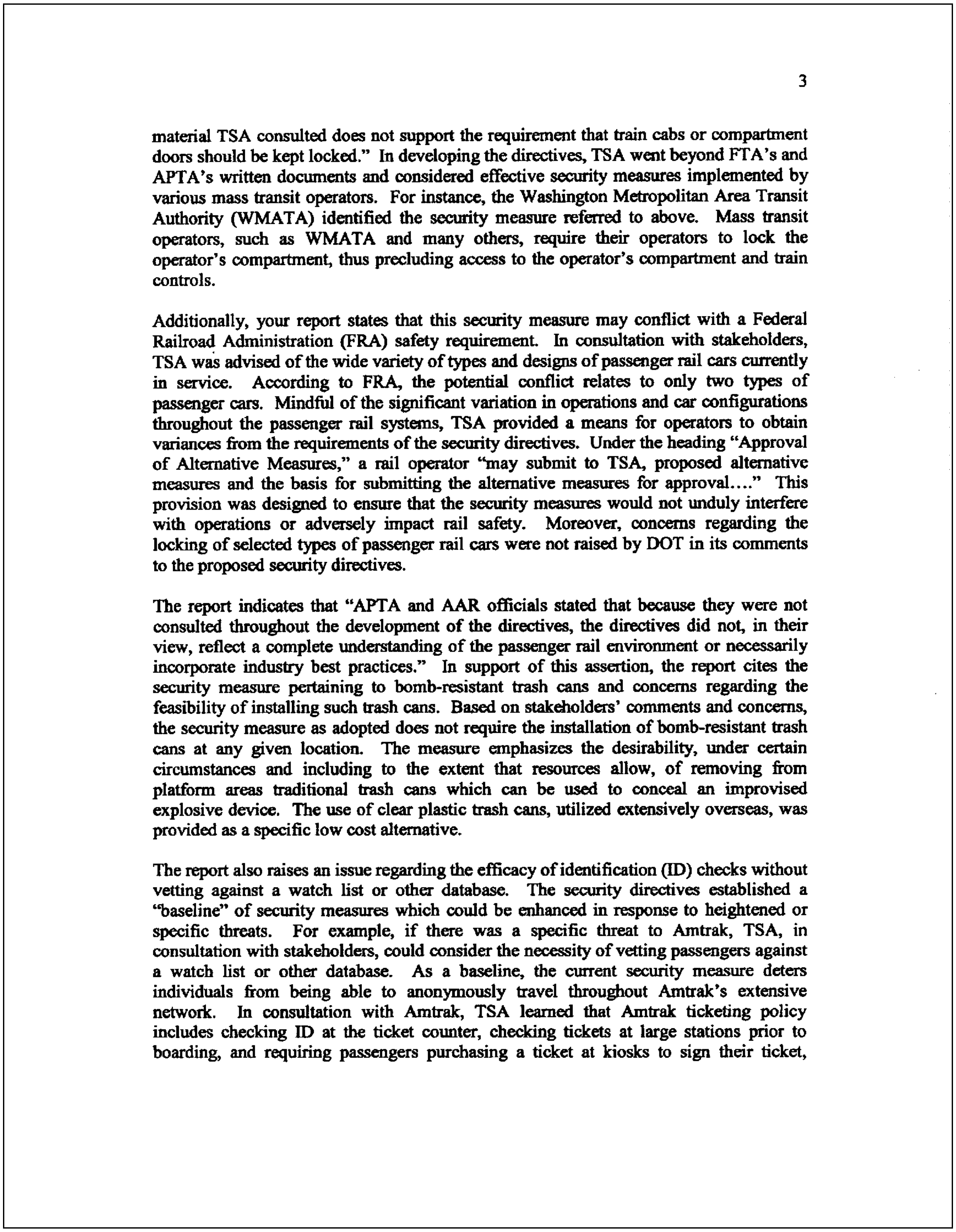
With that being said, we would like to pose some specific comments related to the TSA portion of the report. To be specific, in the section of your draft report entitled, "TSA Has Begun to Assess Risks to Passenger Rail," you comment on the exclusion of industry groups such as the American Public Transportation Association (APTA) and the Association of American Railroads (AAR) in the development of strategic plans. TSA plans to include these stakeholders in the revised National Infrastructure Protection Plan (NIPP)/Transportation Security Specific Plan (TSSP) development process in order to capture industry's input in the TSSP. TSA has also actively participated with both organizations and their members in working together after the London bombings on July 7, 2005.

Additionally, your assertion that TSA missed the deadline for completing the TSSP by December 2004 is misleading because TSA did, in fact, complete a draft TSSP in November 2004. Completion of the draft sector-specific plans depends on the content of the NIPP Base Plan which is currently being revised. The revised NIPP, expected to be issued in late 2005, will address your first recommendation as it contains national guidelines and milestones for conducting sector-specific risk assessments.

In your discussion of TSA's methodology for conducting criticality assessments, you state, "According to TSA officials, their final methodology for conducting criticality assessments did not include DOT modal specialists and trade associations." By design, information supporting our criticality assessments is obtained through open source resources; nevertheless, TSA has involved Federal stakeholders as well as owner/operators during the process to complete our criticality assessments. TSA will conduct facilitated vulnerability assessments with private sector stakeholders which include owner/operators.

In the section entitled, "TSA Issued Mandatory Security Directives to Rail Operators but Faces Challenges Related to Compliance and Enforcement," you state that stakeholders were not given an opportunity to comment on the final draft of the directives. While stakeholders were not provided final copies of the security directives prior to issuance, various stakeholders, including Amtrak, were provided with and commented on each of the security measures contained in the security directives.

Your report further states that TSA developed the directives based upon consultation with the industry and a review of best practices in passenger rail and mass transit systems across the country, and were also based upon FTA and APTA best practices for rail security. The report seems to criticize this approach by stating, "For example, the source

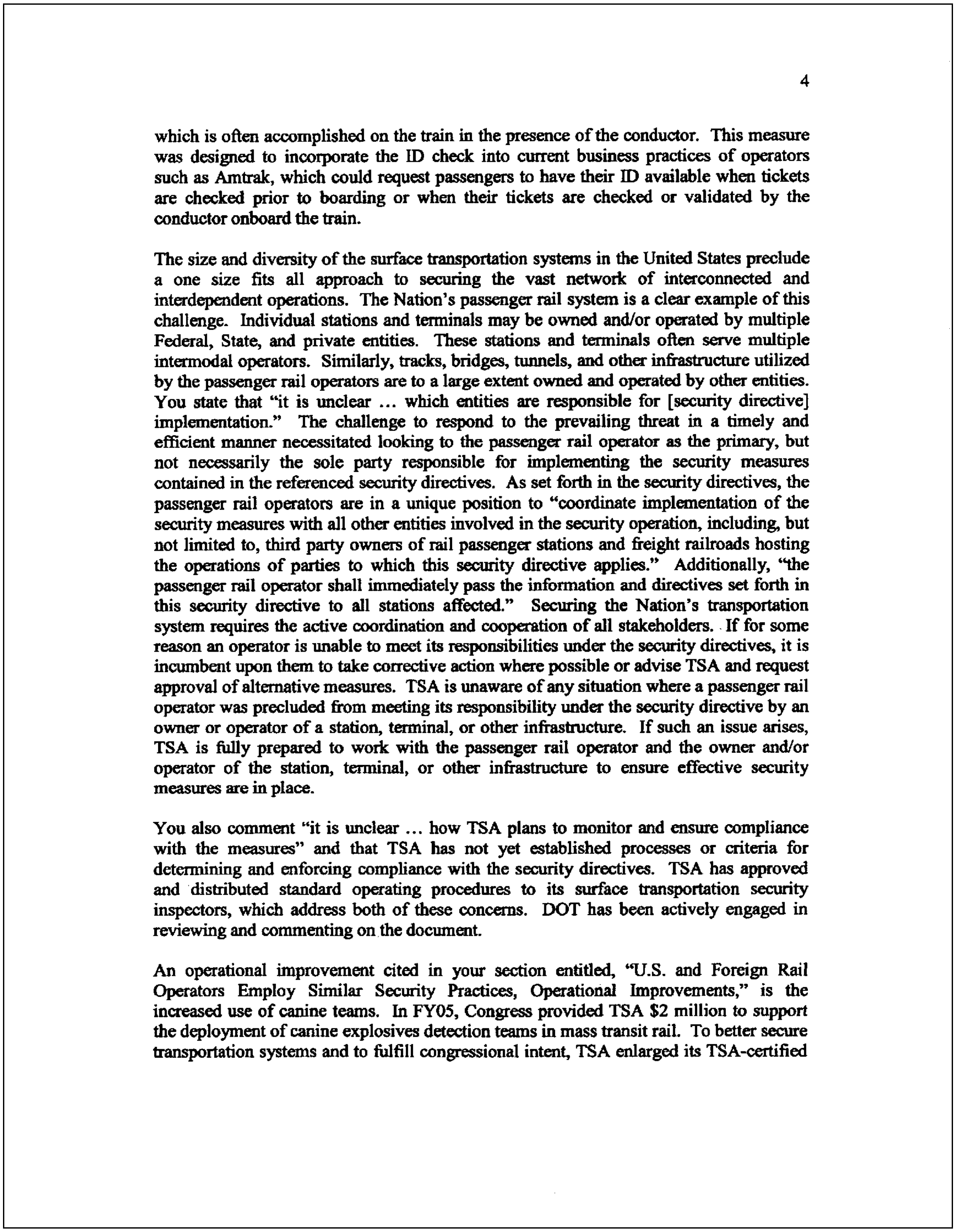


material TSA consulted does not support the requirement that train cabs or compartment doors should be kept locked." In developing the directives, TSA went beyond FTA's and APTA's written documents and considered effective security measures implemented by various mass transit operators. For instance, the Washington Metropolitan Area Transit Authority (WMATA) identified the security measure referred to above. Mass transit operators, such as WMATA and many others, require their operators to lock the operator's compartment, thus precluding access to the operator's compartment and train controls.

Additionally, your report states that this security measure may conflict with a Federal Railroad Administration (FRA) safety requirement. In consultation with stakeholders, TSA was advised of the wide variety of types and designs of passenger rail cars currently in service. According to FRA, the potential conflict relates to only two types of passenger cars. Mindful of the significant variation in operations and car configurations throughout the passenger rail systems, TSA provided a means for operators to obtain variances from the requirements of the security directives. Under the heading "Approval of Alternative Measures," a rail operator "may submit to TSA, proposed alternative measures and the basis for submitting the alternative measures for approval...." This provision was designed to ensure that the security measures would not unduly interfere with operations or adversely impact rail safety. Moreover, concerns regarding the locking of selected types of passenger rail cars were not raised by DOT in its comments to the proposed security directives.

The report indicates that "APTA and AAR officials stated that because they were not consulted throughout the development of the directives, the directives did not, in their view, reflect a complete understanding of the passenger rail environment or necessarily incorporate industry best practices." In support of this assertion, the report cites the security measure pertaining to bomb-resistant trash cans and concerns regarding the feasibility of installing such trash cans. Based on stakeholders' comments and concerns, the security measure as adopted does not require the installation of bomb-resistant trash cans at any given location. The measure emphasizes the desirability, under certain circumstances and including to the extent that resources allow, of removing from platform areas traditional trash cans which can be used to conceal an improvised explosive device. The use of clear plastic trash cans, utilized extensively overseas, was provided as a specific low cost alternative.

The report also raises an issue regarding the efficacy of identification (ID) checks without vetting against a watch list or other database. The security directives established a "baseline" of security measures which could be enhanced in response to heightened or specific threats. For example, if there was a specific threat to Amtrak, TSA, in consultation with stakeholders, could consider the necessity of vetting passengers against a watch list or other database. As a baseline, the current security measure deters individuals from being able to anonymously travel throughout Amtrak's extensive network. In consultation with Amtrak, TSA learned that Amtrak ticketing policy includes checking ID at the ticket counter, checking tickets at large stations prior to boarding, and requiring passengers purchasing a ticket at kiosks to sign their ticket,

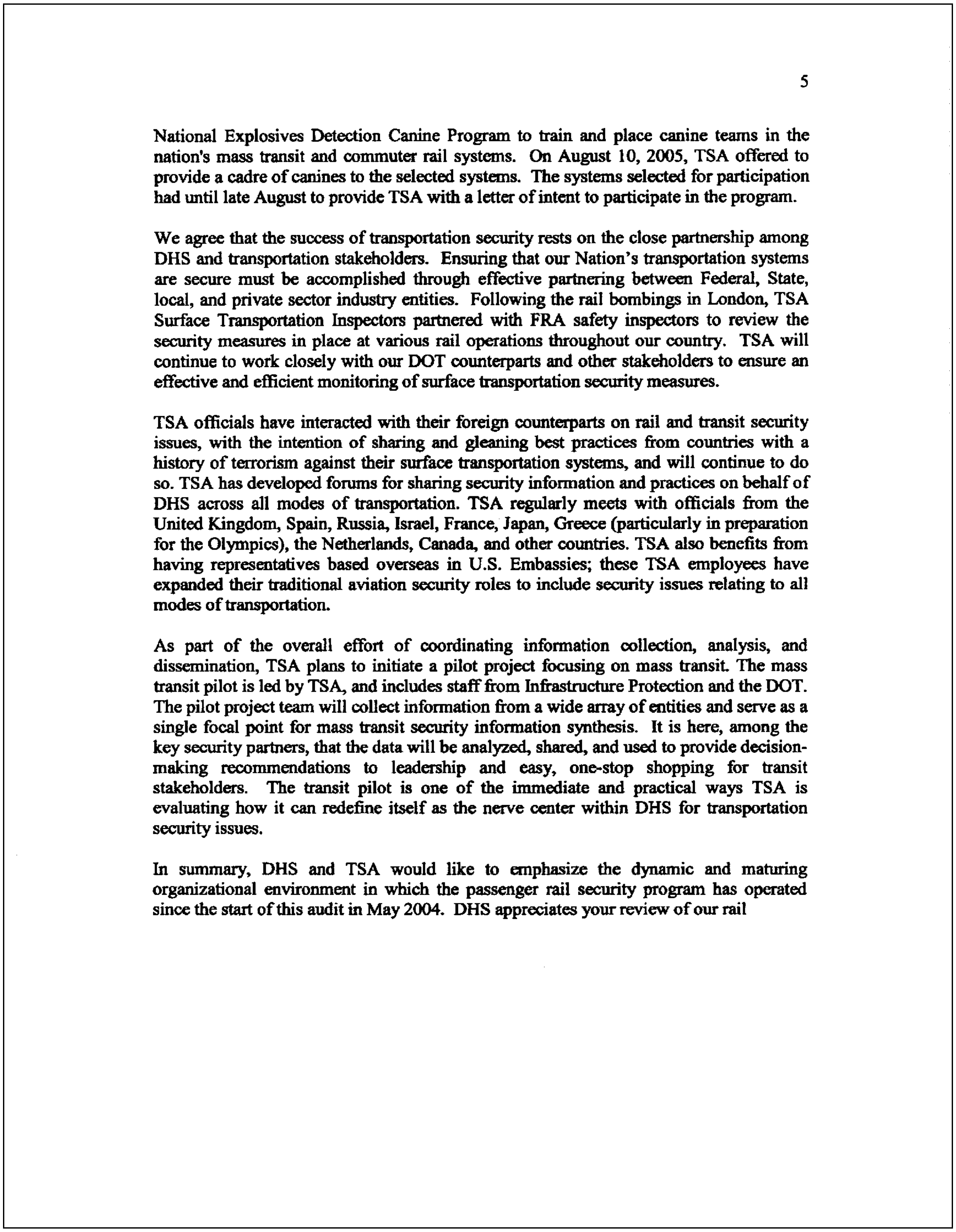


which is often accomplished on the train in the presence of the conductor. This measure was designed to incorporate the ID check into current business practices of operators such as Amtrak, which could request passengers to have their ID available when tickets are checked prior to boarding or when their tickets are checked or validated by the conductor onboard the train.

The size and diversity of the surface transportation systems in the United States preclude a one size fits all approach to securing the vast network of interconnected and interdependent operations. The Nation's passenger rail system is a clear example of this challenge. Individual stations and terminals may be owned and/or operated by multiple Federal, State, and private entities. These stations and terminals often serve multiple intermodal operators. Similarly, tracks, bridges, tunnels, and other infrastructure utilized by the passenger rail operators are to a large extent owned and operated by other entities. You state that "it is unclear … which entities are responsible for [security directive] implementation." The challenge to respond to the prevailing threat in a timely and efficient manner necessitated looking to the passenger rail operator as the primary, but not necessarily the sole party responsible for implementing the security measures contained in the referenced security directives. As set forth in the security directives, the passenger rail operators are in a unique position to "coordinate implementation of the security measures with all other entities involved in the security operation, including, but not limited to, third party owners of rail passenger stations and freight railroads hosting the operations of parties to which this security directive applies." Additionally, "the passenger rail operator shall immediately pass the information and directives set forth in this security directive to all stations affected." Securing the Nation's transportation system requires the active coordination and cooperation of all stakeholders. If for some reason an operator is unable to meet its responsibilities under the security directives, it is incumbent upon them to take corrective action where possible or advise TSA and request approval of alternative measures. TSA is unaware of any situation where a passenger rail operator was precluded from meeting its responsibility under the security directive by an owner or operator of a station, terminal, or other infrastructure. If such an issue arises, TSA is fully prepared to work with the passenger rail operator and the owner and/or operator of the station, terminal, or other infrastructure to ensure effective security measures are in place.

You also comment "it is unclear … how TSA plans to monitor and ensure compliance with the measures" and that TSA has not yet established processes or criteria for determining and enforcing compliance with the security directives. TSA has approved and distributed standard operating procedures to its surface transportation security inspectors, which address both of these concerns. DOT has been actively engaged in reviewing and commenting on the document.

An operational improvement cited in your section entitled, "U.S. and Foreign Rail Operators Employ Similar Security Practices, Operational Improvements," is the increased use of canine teams. In FY05, Congress provided TSA $2 million to support the deployment of canine explosives detection teams in mass transit rail. To better secure transportation systems and to fulfill congressional intent, TSA enlarged its TSA-certified



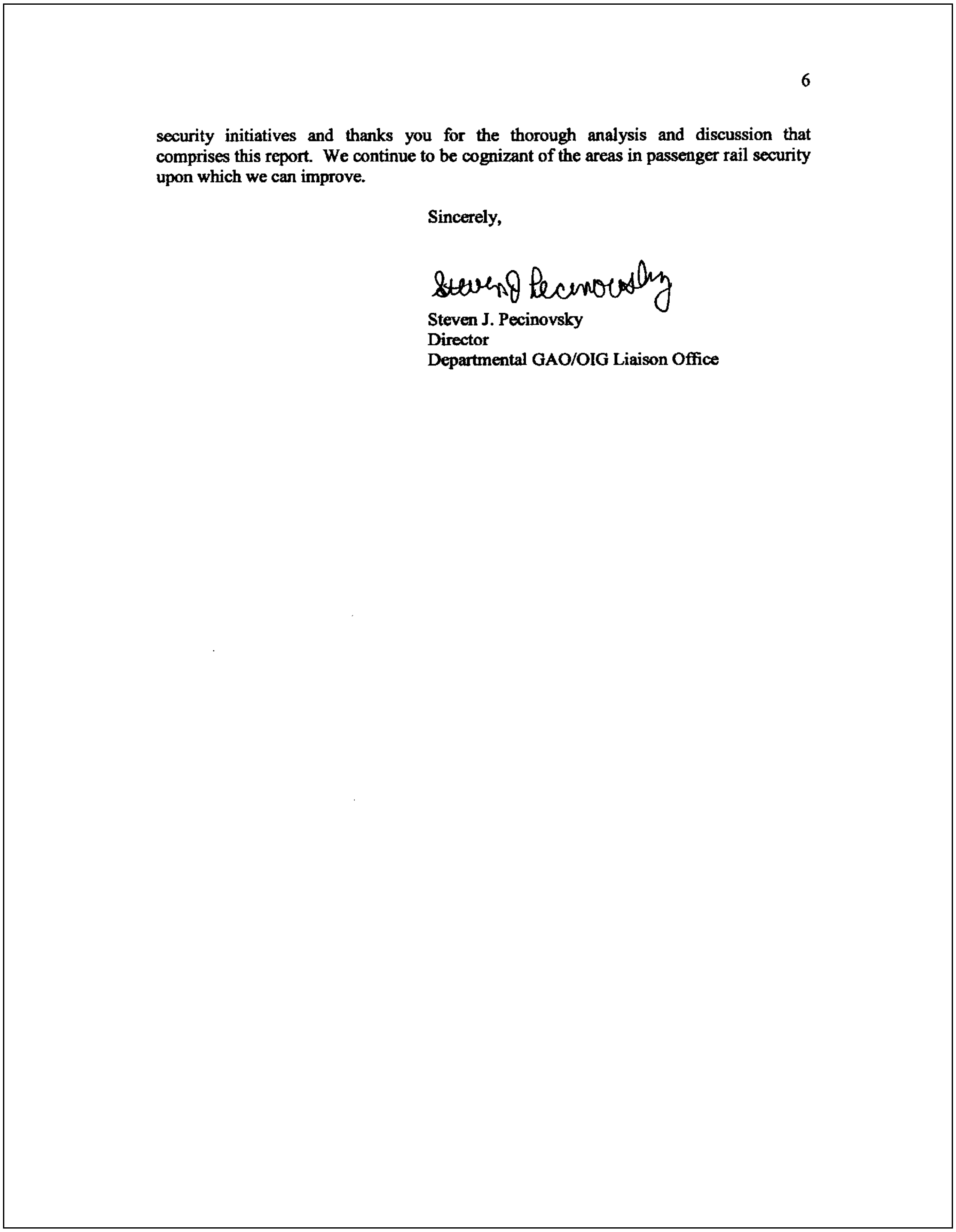
National Explosives Detection Canine Program to train and place canine teams in the nation's mass transit and commuter rail systems. On August 10, 2005, TSA offered to provide a cadre of canines to the selected systems. The systems selected for participation had until late August to provide TSA with a letter of intent to participate in the program.

We agree that the success of transportation security rests on the close partnership among DHS and transportation stakeholders. Ensuring that our Nation's transportation systems are secure must be accomplished through effective partnering between Federal, State, local, and private sector industry entities. Following the rail bombings in London, TSA Surface Transportation Inspectors partnered with FRA safety inspectors to review the security measures in place at various rail operations throughout our country. TSA will continue to work closely with our DOT counterparts and other stakeholders to ensure an effective and efficient monitoring of surface transportation security measures.

TSA officials have interacted with their foreign counterparts on rail and transit security issues, with the intention of sharing and gleaning best practices from countries with a history of terrorism against their surface transportation systems, and will continue to do so. TSA has developed forums for sharing security information and practices on behalf of DHS across all modes of transportation. TSA regularly meets with officials from the United Kingdom, Spain, Russia, Israel, France, Japan, Greece (particularly in preparation for the Olympics), the Netherlands, Canada, and other countries. TSA also benefits from having representatives based overseas in U.S. Embassies; these TSA employees have expanded their traditional aviation security roles to include security issues relating to all modes of transportation.

As part of the overall effort of coordinating information collection, analysis, and dissemination, TSA plans to initiate a pilot project focusing on mass transit. The mass transit pilot is led by TSA, and includes staff from Infrastructure Protection and the DOT. The pilot project team will collect information from a wide array of entities and serve as a single focal point for mass transit security information synthesis. It is here, among the key security partners, that the data will be analyzed, shared, and used to provide decision-making recommendations to leadership and easy, one-stop shopping for transit stakeholders. The transit pilot is one of the immediate and practical ways TSA is evaluating how it can redefine itself as the nerve center within DHS for transportation security issues.

In summary, DHS and TSA would like to emphasize the dynamic and maturing organizational environment in which the passenger rail security program has operated since the start of this audit in May 2004. DHS appreciates your review of our rail



security initiatives and thanks you for the thorough analysis and discussion that comprises this report. We continue to be cognizant of the areas in passenger rail security upon which we can improve.

Sincerely,

Steven J Pecinovsky

Steven J. Pecinovsky
Director
Departmental GAO/OIG Liaison Office

Appendix V: GAO Contacts and Staff Acknowledgments

GAO Contacts

Cathleen A. Berrick, (202) 512-8777
JayEtta Z. Hecker, (202) 512-2834

Acknowledgments

In addition to those named above, Seto Bagdoyan, Amy Bernstein, Leo Barbour, Christopher Currie, Nikki Clowers, Scott Farrow, David Hooper, Andrew Huddleston, Kirk Kiester, Octavia Parks, Jack Schulze, and Ray Sendejas made key contributions to this report.

(440319)

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone:	Voice:	(202) 512-6000
	TDD:	(202) 512-2537
	Fax:	(202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON RECYCLED PAPER