GAO

For Release on Delivery
Expected at 10:00 a.m. EDT
Thursday, October 20, 2005

PASSENGER RAIL SECURITY

Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts

Statement of Cathleen A. Berrick, Director
Homeland Security and Justice Issues

G A O
Accountability ★ Integrity ★ Reliability

GAO-06-181T

PASSENGER RAIL SECURITY

Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts

Why GAO Did This Study

The July 2005 bombing attacks on London's subway system dramatically highlighted the vulnerability of passenger rail systems worldwide to terrorist attacks, and the need for an increased focus on security for these systems.

This testimony provides information on how the Department of Homeland Security (DHS), including the Transportation Security Administration (TSA) and the Office for Domestic Preparedness (ODP), have assessed risks posed by terrorism to the U.S. passenger rail system using risk management principles; actions federal agencies have taken to enhance the security of U.S. rail systems; and rail security practices implemented by domestic and selected foreign passenger rail operators and differences among these practices.

What GAO Recommends

GAO's September 2005 report on passenger rail security recommended, among other things, that TSA develop a timeline for completing its methodology for conducting risk assessments, and develop rail security standards that reflect industry best practices and can be measured and enforced. GAO also recommended that the Secretary of DHS determine the feasibility of implementing certain security practices used by foreign rail operators. DHS, DOT, and Amtrak generally agreed with the report's recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-06-181T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Cathleen A. Berrick at (202) 512-3404 or berrickc@gao.gov.

What GAO Found

Within DHS, ODP has completed numerous risk assessments of passenger rail systems around the country, and TSA has begun to conduct risk assessments as well as establish a methodology for determining how to analyze and characterize risks that have been identified. Until TSA completes these efforts, however, the agency will not be able to prioritize passenger rail assets and help guide security investment decisions. 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.

In addition to the ongoing initiatives to enhance passenger rail security conducted by the Department of Transportation's (DOT) Federal Transit Administration and Federal Railroad Administration, such as providing security training to passenger rail operators, TSA issued emergency security directives in 2004 to domestic rail operators after terrorist attacks on the rail system in Madrid 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 security directives, citing limited opportunities to collaborate with TSA to ensure that industry best practices were incorporated.

Domestic and foreign passenger rail operators we contacted have taken a range of actions to help secure their systems. Most, for example, had implemented customer awareness programs to encourage passengers to report suspicious activities, increased the number and visibility of their security personnel, upgraded security technology, and improved rail system design to enhance security. We also observed security practices among certain foreign passenger rail systems or their governments not currently used by the domestic rail operators we contacted, or by the U.S. government, which could be considered for use in the United States. For example, some foreign rail operators randomly screen passengers or utilize covert testing to help keep employees alert to security threats, and some foreign governments maintain centralized clearinghouses on rail security technologies. While introducing any of these security practices into the U.S. rail system may pose political, legal, fiscal, and cultural challenges, they may nevertheless warrant further examination.

_____ **United States Government Accountability Office**

Mr. Chairman and Members of the Committee:

Thank you for inviting me to participate in today's hearing on passenger and freight rail security. The London rail bombings that took place in July—resulting in over 50 fatalities and more than 700 injuries—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 terrorist attack. While securing the U.S. passenger rail system is a daunting task—a shared responsibility requiring coordinated action on the part of federal, state, and local governments and the private sector—it is important nonetheless to take the necessary steps to identify and mitigate risks to passenger rail systems.

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. Key federal stakeholders with critical roles to play within the rail sector include the Transportation Security Administration (TSA), which is responsible for transportation security overall, and the Office for Domestic Preparedness (ODP), which provides grant funds to rail operators and conducts risk assessments for passenger rail agencies, both within the Department of Homeland Security (DHS); and the Federal Transit Administration (FTA) and Federal Railroad Administration (FRA), both within the Department of Transportation (DOT). One of the critical challenges facing these federal agencies, and rail system operators they oversee or support, is finding ways to protect rail systems from potential terrorist attacks without compromising the accessibility and efficiency of rail travel.

At the federal level, another significant challenge to securing rail systems involves allocation of resources. The U.S. 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.[1] 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 DHS declared that as a core principle of the reorganization, the department must base its work on priorities driven by risk.

My testimony today focuses on 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, and the security practices implemented by foreign passenger rail operators. In particular, my testimony highlights three key areas: (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. My comments today are based upon our recently issued report to Senators Snowe and Boxer of this committee, the chairman of the House Transportation and Infrastructure Subcommittee on Railroads, and Representative Castle.[2]

In summary:

- Within DHS, ODP has completed numerous risk assessments of passenger rail systems around the country, and TSA has begun to conduct risk assessments as well as establish a methodology for determining how to analyze and characterize risks that have been identified. Until TSA completes these efforts, however, or sets

---

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

[2]GAO, *Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts*, GAO-05-851 (Washington, D.C.: Sept. 9, 2005).

timelines for doing so, the agency will not be able to prioritize passenger rail assets and help guide security investment decisions. 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.

- In addition to the ongoing initiatives to enhance passenger rail conducted by the FTA and FRA, in 2004, TSA issued emergency security directives to domestic rail operators after terrorist attacks on the rail system in Madrid 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 these 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 are developing agreements to delineate specific security-related roles and responsibilities, among other things, for the different modes. An agreement for transit security was signed in September 2005.

- Domestic and foreign passenger rail operators we contacted have taken a range of actions to help secure their systems. Most, for example, 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 use of canine teams to detect explosives, enhanced employee training programs, upgraded security technology, tightened access controls, and made rail system design improvements to enhance security. 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, which could be considered for use in the United States. For example, some foreign rail operators randomly screen passengers or utilize covert testing to help keep employees alert to security threats, and some foreign governments maintain centralized clearinghouses on rail security technologies and best practices. While introducing any of these security practices into the U.S. rail system may pose political, legal, fiscal, and cultural challenges, they may nevertheless warrant further examination.

In our September 2005 report on passenger rail security, we recommended, among other things, that 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, TSA should establish a plan with timelines for completing its methodology for conducting risk assessments and develop security standards that reflect industry best practices and can be measured and enforced, by using the federal rule-making process. In addition, we recommended that the Secretary of DHS, in collaboration with DOT and the passenger rail industry, determine the feasibility, in a risk management context, of implementing certain security practices used by foreign rail operators. DHS, DOT, and Amtrak generally agreed with the report's recommendations.

Background

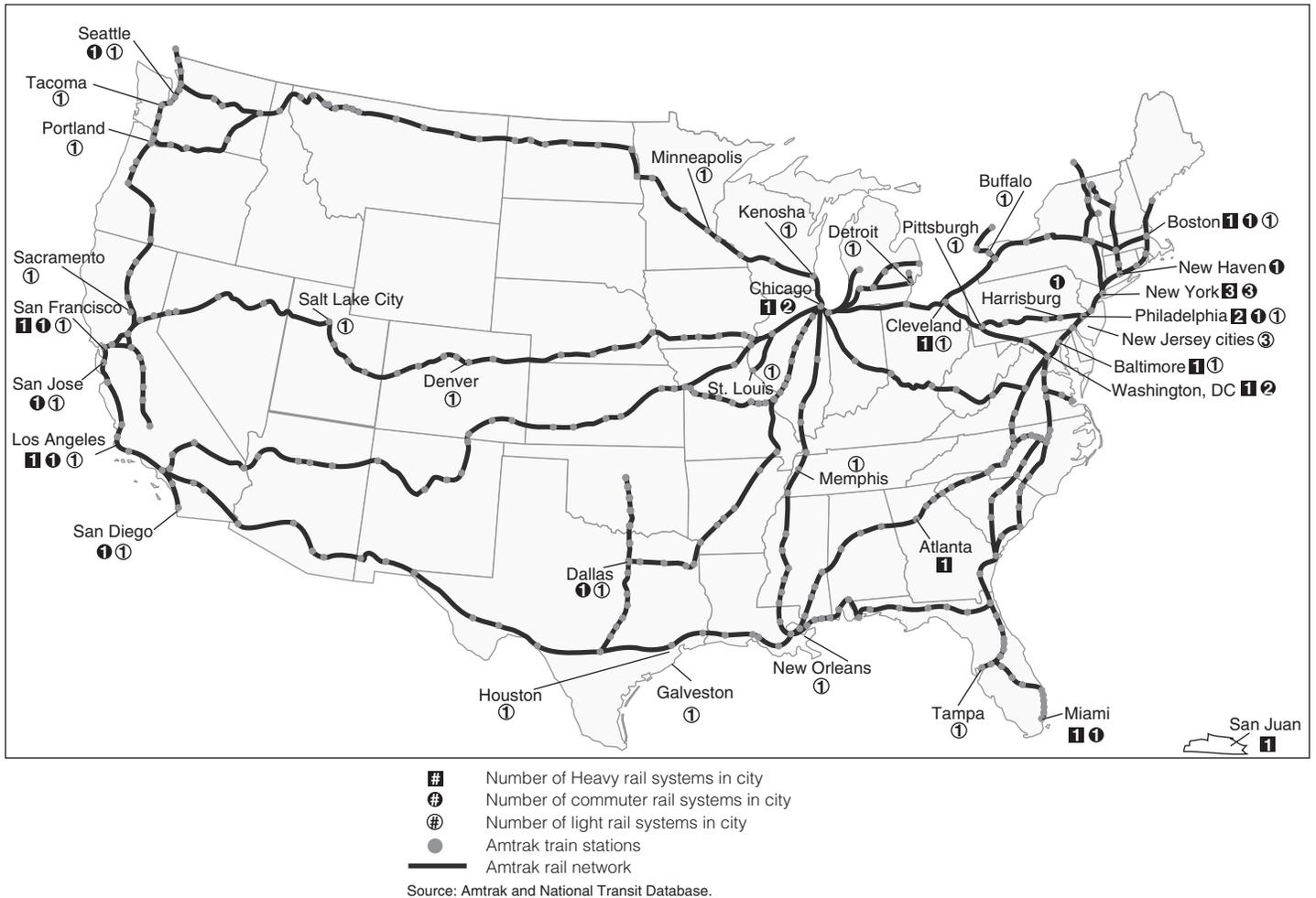## Overview of the Passenger Rail System

Each weekday, 11.3 million passengers in 35 metropolitan areas and 22 states use some form of rail transit (commuter, heavy, or light rail).[3] 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. 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. Amtrak operates the nation's primary intercity passenger rail service over a 22,000-mile network, primarily over leased freight railroad tracks.[4] 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. Figure 1 identifies the geographic location of rail transit systems and Amtrak within the United States.

---

[3]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.

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

Figure 1: Geographic Distribution of Amtrak and Rail Transit Systems

Seattle ❶ ①
Tacoma ①
Portland ①
Minneapolis ①
Kenosha ①
Detroit ①
Buffalo ①
Pittsburgh ①
Boston ■ ❶ ①
New Haven ❶
New York ■ ❸
Harrisburg ❶
Philadelphia ■ ❶ ①
New Jersey cities ③
Cleveland ■ ①
Baltimore ■ ①
Washington, DC ■ ❷
Chicago ■ ❷
Sacramento ①
San Francisco ■ ❶ ①
Salt Lake City ①
Denver ①
St. Louis ①
San Jose ❶ ①
Los Angeles ■ ❶ ①
Memphis ①
San Diego ❶ ①
Atlanta ■
Dallas ❶ ①
New Orleans ①
Houston ①
Galveston ①
Tampa ①
Miami ■ ❶
San Juan ■

Symbol	Description
■	Number of Heavy rail systems in city
❶	Number of commuter rail systems in city
①	Number of light rail systems in city
●	Amtrak train stations
▬▬	Amtrak rail network

Source: Amtrak and National Transit Database.

Passenger Rail Systems Are Inherently Vulnerable to Terrorist Attacks

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

Multiple Stakeholders Share Responsibility for Security 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.[5] 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.[6]

With the creation of DHS in 2002, one of its components, ODP, became primarily responsible for overseeing security funding for passenger rail

---

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

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

systems.[7] 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 conducting risk analysis and risk management activities of state and local governments.[8] 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. The DHS Appropriations Act of 2005 appropriated $150 million for rail transit, intercity passenger rail, freight rail, and transit agency security grants.[9] With this funding, ODP created and is administering two grant 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 systems.

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. FRA has regulatory authority for rail safety over commuter rail operators and Amtrak, and

---

[7]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.

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

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

employs over 400 rail inspectors that periodically monitor the implementation of safety and security plans at these systems.[10]

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 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. 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.

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),[11] 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

---

[10]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.

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

objectives, performing risk assessments, evaluating alternative actions to reduce identified risks by preventing or mitigating their impact, management selecting actions to undertake, 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
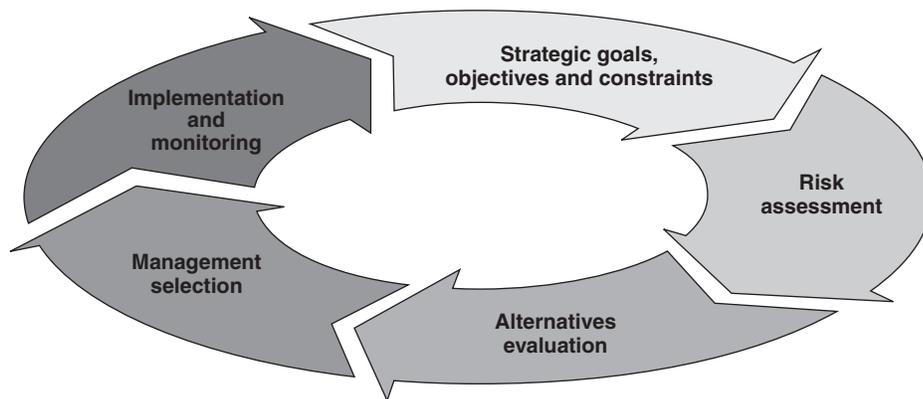
Source: GAO.

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.[12] 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.

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

---

[12]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).

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 policies, 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.[13] These agencies are responsible for infrastructure 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.[14] 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 National Infrastructure Protection Plan 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

---

[13]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.

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

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.

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.[15] Twelve additional risk assessments are under way, and an additional 11 passenger rail operators have requested assistance through this program. The results developed in

---

[15]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.

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 that, accordingly, are likely candidates for early risk mitigation action.

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-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.[16] 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. According to authority officials, the risk assessment that was conducted 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.

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.

---

[16]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.

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 FRA, TSA, the American Association of Railroads (AAR), and others to develop a risk assessment tool for freight rail corridors.[17] 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. 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.[18] 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.

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 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

---

[17]The Association of American 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.

[18]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.

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.[19] 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

In October 2004, TSA completed an overall threat assessment for both mass transit and passenger and freight rail modes.[20] 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.

---

[19]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.

[20]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 testimony.

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, 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 3 illustrates the overall progress TSA had made in conducting risk assessments for passenger rail assets as of July 2005.

Figure 3: Status of TSA's Passenger Rail Risk Assessment Efforts, as of July 2005
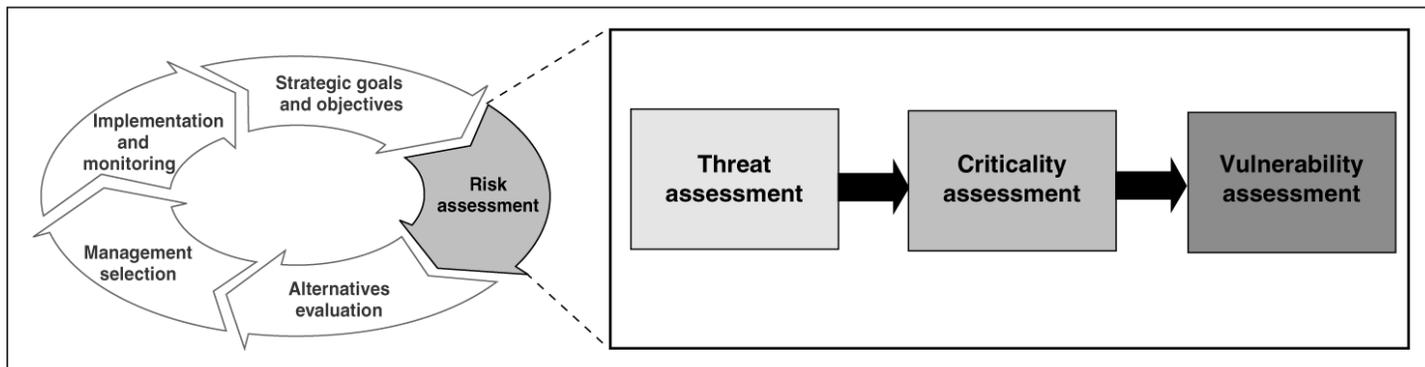
Source: GAO.

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 not yet produced the TSSP required by HSPD-7 to be issued in December of 2004, though a draft was prepared in November 2004. 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.

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.[21] 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

---

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

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—had not yet been 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 been finalized or provided to TSA or other sector-specific agencies, it is not 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 after September 11. FTA, using an $18.7 million appropriation by the Department of Defense and Emergency Supplemental Appropriations Act of 2002, launched a multipart transit security initiative, much of which is still in place. The initiative included security readiness assessments, technical assistance, grants for emergency response drills, and training. For example, 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. 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. In addition, FTA has issued guidance, such as its Top 20 Security Program Action Items for Transit Agencies, which recommends measures for passenger rail operators to implement into their security programs to improve both security and emergency preparedness.

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.

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.[22] 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 1 contains examples of security measures required by these directives.

---

[22]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.

Table 1: 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 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 it 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[23] 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 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

---

[23]49 CFR 238.235.

compliance with the security directives. As of July 2005, TSA had hired 57 of up to 100 inspector positions authorized by Congress.[24] 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 nonspecific 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 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

---

[24]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.

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 that 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 4 summarizes TRIP's three-phased approach.

Figure 4: 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 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 response to a previous recommendation we made in a June 2003 report on transportation security, DHS and DOT signed a memorandum of understanding (MOU) 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 critical infrastructure. 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. The annex for mass transit security was signed in September 2005.[25] According to DHS and DOT officials, this annex is intended to ensure that the programs and protocols for incorporating stakeholder feedback and making enhancements to security measures are coordinated. For example, the annex requires that DHS and DOT consult on such matters as regulations

---

[25]Congress required that an annex to the MOU be signed that would, among other things, define and clarify the respective transit security roles and responsibilities of each department. Pub. L. 109-59, § 3028 (2005).

and security directives that affect security and identifies points of contact for coordinating this consultation.

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.[26]

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.[27]

---

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

[27]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.

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 direct contact or during industry association meetings.[28] 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

---

[28]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.

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.

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

Both U.S. and foreign passenger rail operators we contacted have implemented similar improvements to enhance the security of their systems.[29] A summary of these efforts follows.

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. 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.

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.

---

[29]Actions taken by Amtrak to enhance security are discussed later in this testimony.

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.

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, and may be called in when a suspicious package is detected. 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. As in the United States, and in contrast to Asia, most European passenger rail operators 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. 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. 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.

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.

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.

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. 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.

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. All 13 foreign operators had implemented some form of access control to their critical facilities or rights-of-way. 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.

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. 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.

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.

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 5 for a photograph of a help post.

Figure 5: 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. In addition, 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.

Figure 6 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.

Figure 6: Composite of Selected Security Practices in the Passenger Rail Environment
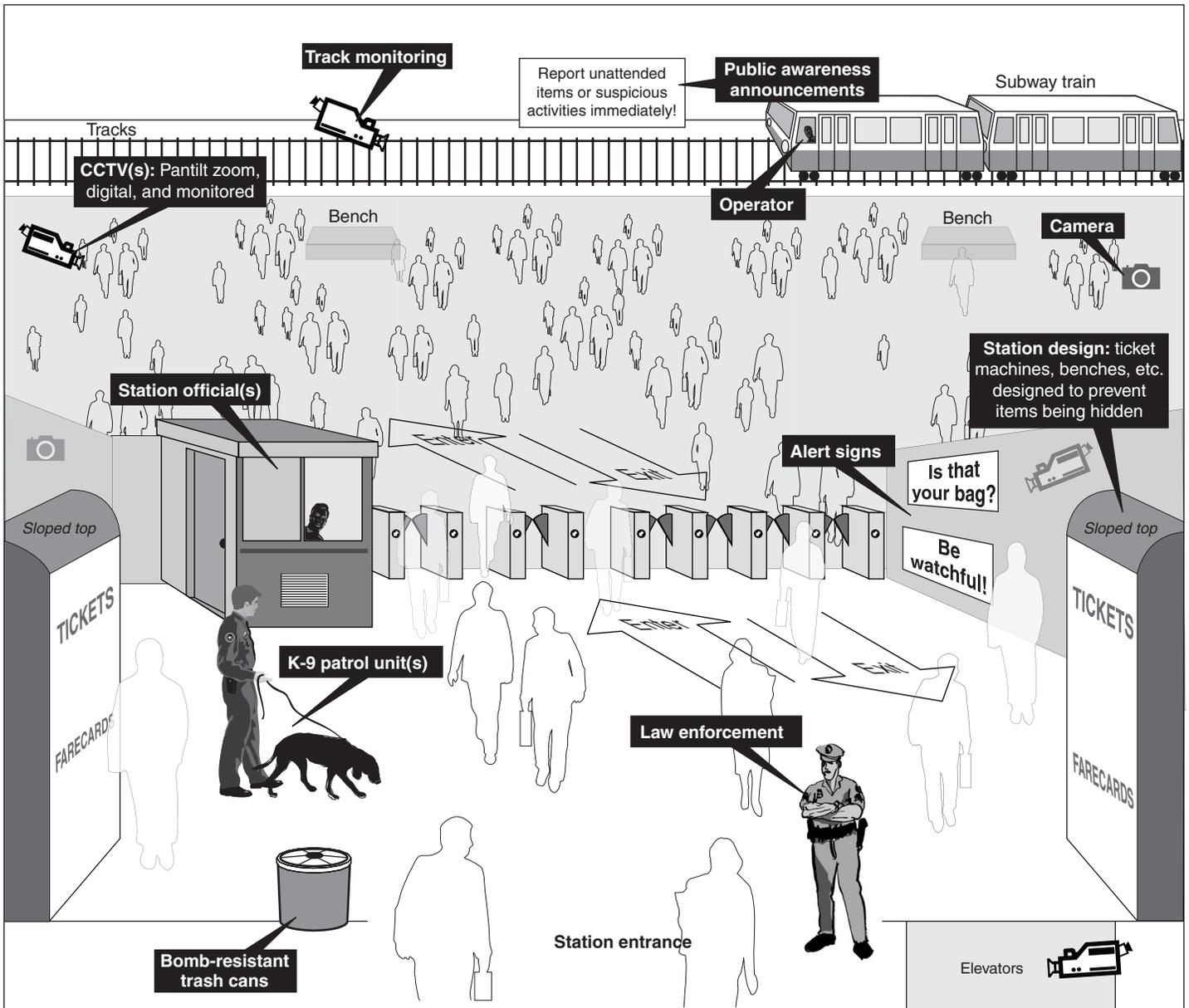
Security resources currently used

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.

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 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 currently expects to finish by December 31, 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 as of 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. 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. 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.

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. 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 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.[30] 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.[31]

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

---

[30]GAO-03-843.

[31]See GAO-03-843.

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 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 (Régie 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 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.[32] Rather, some transit agencies maintain individual polices forces, while others rely on their city or county police forces for security.

Conclusions

In conclusion, Mr. Chairman, 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. However, enhanced federal leadership is needed to help ensure that actions and investments designed to enhance security are properly focused and prioritized, so that finite resources may be allocated appropriately to help protect all modes of transportation and secure other

---

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

national critical infrastructure sectors. Leadership on this issue should reflect the shared responsibilities required to coordinate actions on the part of federal, state, and local governments; the private sector; and rail passengers who ride these systems.

Specifically, 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 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.

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.

In our recently issued report on passenger rail security, we recommended, among other things, that 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, TSA should establish a plan with timelines for completing its methodology for conducting risk assessments and develop security standards that reflect industry best practices and can be measured and enforced, by using the federal rule-making process. In addition, we recommended that the Secretary of DHS, in collaboration with DOT and the passenger rail industry, determine the feasibility, in a risk management context, of implementing certain security practices used by foreign rail operators. DHS, DOT, and Amtrak generally agreed with the report's recommendations.

Mr. Chairman, this concludes my statement. I would be pleased to answer any questions that you or other members of the Committee may have at this time.

Contact Information

For further information on this testimony, please contact Cathleen A. Berrick at (202) 512-3404 or JayEtta Z. Hecker at (202) 512-2834. Individuals making key contributions to this testimony include Seto Bagdoyan, Amy Bernstein, Leo Barbour, Christopher Currie, Nikki Clowers, David Hooper, Kirk Kiester, and Ray Sendejas.