United States Government Accountability Office

GAO

Testimony before the Subcommittee on Transportation Security and Infrastructure Protection, Committee on Homeland Security, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EST
Tuesday, February 6, 2007

PASSENGER RAIL SECURITY

Federal Strategy and Enhanced Coordination Needed to Prioritize and Guide Security Efforts

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

February 6, 2007

PASSENGER RAIL SECURITY

Federal Strategy and Enhanced Coordination Needed to Prioritize and Guide Security Efforts

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-07-442T, a testimony before the Subcommittee on Transportation Security and Infrastructure Protection, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

The 2005 London subway bombings and 2006 rail attacks in Mumbai, India highlighted the vulnerability of passenger rail and other surface transportation systems to terrorist attack and demonstrated the need for greater focus on securing these systems. This testimony is based primarily on GAO's September 2005 passenger rail security report and selected program updates obtained in January 2007. Specifically, it addressees (1) the extent to which the Department of Homeland Security (DHS) has assessed the risks facing the U.S. passenger rail system and developed a strategy based on risk assessment for securing all modes of transportation, including passenger rail; (2) the actions that the Transportation Security Administration (TSA) and other federal agencies have taken to enhance the security of the U.S. passenger rail system, improve federal coordination, and develop industry partnerships; and (3) the security practices that domestic and selected foreign passenger rail operators have implemented to enhance security.

What GAO Recommends

We have previously recommended that TSA complete risk assessments, develop rail security standards based on best practices, and consider implementing practices used by foreign rail operators. DHS, Department of Transportation (DOT), and Amtrak generally agreed with these recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-07-442T.

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

What GAO Found

The DHS Office of Grants and Training and TSA have begun to assess the risks facing the U.S. passenger rail system. However, we reported in September 2005 that TSA had not completed a comprehensive risk assessment of passenger rail assets. We found that, until TSA does so, the agency may be limited in its ability to prioritize passenger rail assets and help guide security investments. We also reported that DHS had begun, but not yet completed, a framework to help agencies and the private sector develop a consistent approach for analyzing and comparing risks among and across various critical sectors. Since that time, TSA has reported taking additional steps to assess the risks to the passenger rail system. However, TSA has not yet issued the required Transportation Sector Specific Plan and supporting plans that address passenger rail and other surface transportation modes, based on a risk assessment. Until TSA does so, the agency lacks a clear strategy with goals and objectives for securing the overall transportation sector, including passenger rail.

After September 11, DOT initiated efforts to strengthen passenger rail security. TSA has also taken actions to strengthen rail security, including issuing security directives, testing security technologies, developing security training, and issuing a proposed rule for passenger and freight rail security, among other efforts. However, federal and rail industry stakeholders have questioned the extent to which TSA's directives were based on industry best practices. TSA has also taken steps to better coordinate with DOT and develop partnerships with industry stakeholders. DHS and DOT have updated their memorandum of understanding to clarify their respective security-related roles and responsibilities for passenger rail. TSA also established an Office of Transportation Sector Network Management and offices for each mode of transportation to develop security policies and work to strengthen partnerships with industry stakeholders for passenger rail and other surface modes.

U.S. and foreign passenger rail operators GAO visited have also taken actions to secure their rail systems. Most had implemented customer security awareness programs, increased security personnel, increased the use of canines to detect explosives, and enhanced employee training programs. GAO also observed security practices among foreign passenger rail systems that are not currently used by U.S. rail operators or by the U.S. government, which could be considered for use in the U.S. For example, some foreign rail operators randomly screen passengers or use covert testing to help keep employees alert to security threats. While introducing these security practices in the U.S may pose political, legal, fiscal, and cultural challenges, they warrant further examination. TSA has reported taking steps to identify foreign best practices for rail security.

Madam Chairwoman and Members of the Subcommittee:

Thank you for inviting me to participate in today's hearing on federal rail and public transportation security efforts. Since September 11, 2001, TSA has focused much of its efforts and resources on meeting legislative mandates to strengthen commercial aviation security. However, TSA has recently placed additional focus on securing surface modes of transportation, particularly in the area of passenger rail. Surface modes of transportation, which include passenger and freight rail, mass transit, highways, including commercial vehicles, and pipelines, are inherently open and difficult to secure. One of the critical challenges facing federal agencies and the rail system operators they oversee or support is finding ways to protect these systems from potential terrorist attacks without compromising the accessibility and efficiency of rail travel. The Madrid commuter rail attacks in March 2004, London rail bombings in July 2005, and Mumbai, India train bombings just last year, highlight the vulnerabilities of passenger rail and other surface transportation systems and made clear that even when security precautions are put into place, these systems remain vulnerable to attack. Securing rail and surface transportation systems is a daunting task, requiring that the federal government develop a clear strategy, including goals and objectives, for strengthening the security of these systems. As part of that strategy, it is also critical to assess the risks facing these systems so that limited resources and security efforts can be prioritized to the areas of greatest need. Furthermore, because the responsibility for securing rail and other transportation modes is shared between federal, state, and local governments and the private sector, it is critical that the federal government develop partnerships and coordinate its security efforts with transportation industry stakeholders.

As we have reported previously, the sheer number of stakeholders involved in securing surface transportation modes, including passenger rail, can sometimes lead to communication challenges, duplication of effort, and confusion about roles and responsibilities. Regarding passenger rail security, key Department of Homeland Security (DHS) stakeholders with critical roles include the Transportation Security Administration (TSA), which is responsible for the security of all modes of transportation, including developing a national strategy and plan for securing the transportation sector as well as supporting plans for each transportation mode. In addition, the DHS Office for Grants and Training (OGT) provides grant funds to rail operators and conducts risk assessments for passenger rail agencies. Within the Department of Transportation (DOT), the Federal Transit Administration (FTA) and Federal Railroad Administration (FRA)

have responsibilities for passenger and freight rail safety and security. In addition, public and private passenger rail operators are also responsible for securing their rail systems.

At the federal level, another significant challenge related to securing passenger rail systems involves allocating resources based on risk. Within and among all modes of transportation, there is competition for resources, as federal, state, and local agencies and transportation 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 the areas of greatest risk within and among 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 Intelligence Reform and Terrorism Prevention Act of 2004 provides that a risk management approach be employed to guide decision making related to homeland security resources. 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.

My testimony today focuses on the progress federal agencies and domestic passenger rail operators have made in developing and implementing security strategies and setting security priorities in the wake of September 11, 2001, terrorist attacks, and the security practices implemented by foreign passenger rail operators. In particular, my testimony highlights three key areas: (1) the extent to which DHS has assessed the risks facing the U.S. passenger rail system and developed a strategy based on risk assessment for securing all modes of transportation, including passenger rail; (2) the actions that TSA and other federal agencies have taken to enhance the security of the U.S. passenger rail system, improve federal coordination, and develop industry partnerships; and (3) the security practices that domestic and selected foreign passenger rail operators have

implemented to enhance security. My comments today are based on GAO's September 2005 report addressing the security of the U.S. passenger rail system.[1] This report was based on work conducted at DHS, DOT, and Amtrak, as well as 32 passenger rail operators in the U.S., and 13 passenger rail operators in 7 European and Asian countries. In addition, in January 2007, we obtained selected updates from DHS regarding its efforts to secure passenger rail systems. We conducted our work in accordance with generally accepted government auditing standards.

We have been requested by this Committee to conduct a follow-on review of passenger rail security, which we expect to initiate in the near future. In addition, we have been requested to assess the security of other surface modes of transportation—including freight rail, commercial vehicles, and highway infrastructure—which we have underway or will initiate later this year.

In Summary

DHS has made progress in assessing the risks facing the U.S. passenger rail system, but has not completed a plan based on that risk assessment for securing the entire transportation sector as required by the National Infrastructure Protection Plan and supporting plans for each mode of surface transportation, including passenger rail. The DHS OGT has developed and conducted risk assessments of passenger rail systems to identify and protect rail assets that are vulnerable to attack, such as stations and bridges. TSA has also conducted risk assessments, including a threat assessment of mass transit and passenger rail and assessments of individual critical rail assets. However, we reported in September 2005 that while TSA had begun to establish a methodology for determining how to analyze and characterize the risks identified, the agency had not completed a comprehensive risk assessment of the passenger rail system. We found that, until TSA completed this effort, the agency may be limited in its ability to prioritize passenger rail assets and help guide security investment decisions about protecting them. Since that time, TSA reported that it is working with rail transit agencies to update risk assessments that FTA and FRA conducted after September 11. TSA expects the 50 largest rail transit agencies to complete security self assessments in early 2007. According to TSA, the agency is using the results of these assessments to set priorities, and has identified underground and underwater rail

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

infrastructure and high density passenger rail stations as assets at highest risk. In addition, at the time of our report, DHS had begun developing, but had not yet completed, a framework to help federal agencies and the private sector develop a consistent approach for analyzing and comparing risks to transportation and other critical sectors. Furthermore, TSA has not yet issued a Transportation Sector Specific Plan (TSSP) and supporting plans for rail and other modes of surface transportation, as required by DHS's National Infrastructure Protection Plan and a December 2006 Executive Order. Until TSA issues the TSSP and modal plans, the agency lacks a clear strategy with goals and objectives for securing the overall transportation sector, including passenger rail.

Before and after September 11, 2001, FTA and FRA undertook a number of initiatives to enhance passenger rail security, including conducting security readiness assessments, providing grants for emergency response drills and training, and developing security awareness programs for rail passengers and employees. However, we reported in September 2005 that TSA's coordination efforts with DOT and industry stakeholders related to passenger rail security could be improved. In March 2004, after terrorist attacks on the rail system in Madrid, TSA issued security directives for passenger rail and mass transit. These directives were intended to establish standard protective measures for all passenger rail operators, including Amtrak. However, federal and rail industry stakeholders questioned the extent to which these directives were based on industry best practices and expressed confusion about how TSA would monitor compliance with the directives. In the 16 months since the completion of our work, TSA has reported taking additional actions to strengthen the security of the passenger rail system. For example, TSA has tested rail security technologies, developed training tools for rail workers, and issued a proposed rule in December 2006 regarding passenger and freight rail security, among other efforts. TSA has also taken steps to better coordinate with DOT regarding rail security roles and responsibilities and develop partnerships with industry stakeholders. The memorandum of understanding between DHS and DOT was updated to include specific agreements between TSA and FTA in September 2005, and between TSA and FRA in September 2006, to delineate security-related roles and responsibilities, among other things, for passenger rail and mass transit. In addition, TSA established an Office of Transportation Sector Network Management and offices for each mode of transportation to develop security policies and partnerships with industry stakeholders, including passenger rail and other surface transportation modes.

Domestic and foreign passenger rail operators we contacted during our prior work on passenger rail security had taken a range of actions to secure their systems. Most had implemented customer awareness programs to encourage passengers to remain vigilant and report suspicious activities, increased the number and visibility of 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 were not used, or used to the same degree, by the domestic rail operators we contacted or by the U.S. government which could be considered for use in the U.S. For example, we found that some foreign rail operators randomly screened passengers or utilized covert testing to help keep employees alert to security threats, and some foreign governments maintained 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 nevertheless warrant further examination. Since our report on passenger rail security was issued, TSA has reported taking steps to coordinate with foreign passenger rail operators and governments to identify security best practices. In addition, in January 2007, a TSA official stated that the agency was developing a clearinghouse of transportation security technologies, but a completion date for this effort was not currently available.

In our September 2005 report on passenger rail security, we recommended, among other things, that TSA 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. These actions should help ensure that the federal government has the information it needs to prioritize passenger rail assets based on risk, and evaluate, select, and implement measures to help the passenger rail operators protect their systems against terrorism. 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. However, as of February 2007, DHS has not provided a formal response indicating if or how it has implemented these 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).[2] Commuter rail systems typically operate on railroad tracks and provide regional service 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 freight railroad tracks. 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 during FY 2005.

Passenger Rail Systems Are Inherently Vulnerable to Terrorist Attacks

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, have multiple access points, are hubs serving multiple carriers, and, in some cases, have 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 (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 disrupt scheduled service. In addition, multiple

[2]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.

access points along extended routes could make the cost of securing each location prohibitive. Balancing the potential economic impact of security enhancements with the benefits of such measures is a difficult challenge.

Multiple Stakeholders Share Responsibility for Securing Passenger Rail Systems

Securing the nation's passenger rail systems is a shared responsibility requiring coordinated action on the part of federal, state, and local governments; the private sector; and rail passengers who ride these systems. Since the September 11th attacks, the role of federal agencies in securing the nation's transportation systems, including passenger rail, have continued to evolve. Prior to September 11th, FTA and FRA, within DOT, were the primary federal entities involved in passenger rail security matters. In response to the attacks of September 11th, Congress passed the Aviation and Transportation Security Act (ATSA), which created TSA within DOT and defined its primary responsibility as ensuring the security of all modes of transportation, although its provisions focus primarily on aviation security.[3] The act also gives TSA regulatory authority for security over all transportation modes. 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.[4] The Intelligence Reform and Terrorism Prevention Act of 2004 requires the Secretary of Homeland Security, working jointly with the Secretary of Transportation, to develop a National Strategy for Transportation Security and transportation modal security plans.[5] TSA issued the National Strategy for Transportation Security in 2005. In addition, the DHS National Infrastructure Protection Plan (NIPP) required the development of a Transportation Sector Specific Plan. In accordance with the NIPP, a December 2006 Executive Order required the Secretary of Homeland Security to develop a TSSP by December 31, 2006, and supporting plans for each mode of surface transportation not later than 90 days after completion of the TSSP.[6] According to the NIPP, sector specific plans should, among other things, define the goals and objectives to secure the sector, assess the risks facing

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

[4]See Pub. L. No. 107-296 § 403, 116 Stat. 2135, 2178 (2002).

[5]Pub. L. No. 108-458, §4001, 118 Stat. 3638, 3710-12 (codified at 49 U.S.C. § 114(t)).

[6] On December 5, 2006, the President issued Executive Order 13416, which requires among other things, that DHS develop a comprehensive transportation systems sector specific plan, as defined in the NIPP, not later than December 31, 2006. See 71 Fed. Reg. 71,033 (Dec. 7, 2006).

the sector, identify the critical assets and infrastructure and develop programs to protect them, and develop security partnerships with industry stakeholders within the sector. As of February 2007, TSA had not yet completed the TSSP or the supporting plans for each surface transportation mode.

Within DHS, OGT, formerly the Office for Domestic Preparedness (ODP), has become the federal source for security funding of passenger rail systems.[7] OGT is the principal component of DHS responsible for preparing the United States against 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. In carrying out its mission, OGT 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. OGT 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 passenger rail and transit systems. During fiscal year 2006, OGT provided $110 million to passenger rail transit agencies through the Transit Security Grant Program and about $7 million to Amtrak through the Intercity Passenger Rail Security Grant Program. During fiscal year 2007, OGT plans to distribute $156 million of for rail and bus security grants and $8 million to Amtrak.

While TSA is the lead federal agency for ensuring the security of all transportation modes, FTA conducts safety and security activities,

[7]OGT originated within the Department of Justice's Office of Justice Programs in 1998 as the Office for Domestic Preparedness (ODP). Pursuant to the Homeland Security Act of 2002, ODP was transferred to DHS in March 2003. See Pub. L. No. 107-296, § 403(5), 116 Stat. at 2178 (codified at 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. Recently, SLGCP was incorporated under the Preparedness Directorate as OGT. Pursuant to the Department of Homeland Security Act, 2007, OGT is to be transferred, along with certain other components of the Preparedness Directorate, into the Federal Emergency Management Agency effective March 31, 2007. Pub. L. No. 109-295, § 611(13), 120 Stat. 1355, 1400 (2006)."

including 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 employs over 400 rail inspectors that periodically monitor the implementation of safety and security plans at these systems.[8]

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. 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 passenger rail operators.

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

Risk management is a tool for informing policy makers' decisions about assessing risks, allocating resources, and taking actions under conditions of uncertainty. In recent years, the President, through Homeland Security Presidential Directives (HSPD), and Congress, through the Intelligence Reform and Terrorism Prevention Act of 2004, provided for federal agencies with homeland security responsibilities to apply risk-based principles to inform their decision making regarding allocating limited resources and prioritizing security activities. The 9/11 Commission recommended that the U.S. government should identify and evaluate the transportation assets that need to be protected, set risk-based priorities for defending them, select the most practical and cost-effective ways of doing so, and then develop a plan, budget, and funding to implement the

[8]FRA administers and enforces federal laws and 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 pursuant to 49 U.S.C. § 20103.

effort.[9] We have previously reported that a risk management approach can help to prioritize and focus the programs designed to combat terrorism. Risk management, as applied in the homeland security context, can help federal decision-makers determine where and how to invest limited resources within and among the various modes of transportation.

The Homeland Security Act of 2002 also directed the department's Directorate of Information Analysis and Infrastructure Protection to use risk management principles in coordinating the nation's critical infrastructure protection efforts.[10] This includes integrating relevant information, analysis, and vulnerability assessments to identify 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 and the Intelligence Reform and Terrorism Prevention Act of 2004 further define and establish critical infrastructure protection responsibilities for DHS and those federal agencies given responsibility for particular industry sectors, such as transportation. In June 2006, DHS issued the NIPP, which named TSA as the primary federal agency responsible for coordinating critical infrastructure protection efforts within the transportation sector.[11] In fulfilling its responsibilities under the NIPP, TSA must conduct and facilitate risk assessments in order to identify, prioritize, and coordinate the protection of critical transportation systems infrastructure, as well as develop risk based priorities for the transportation sector.

To provide guidance to agency decision makers, we have created a risk management framework, which is intended to be a starting point for

[9]National Commission on Terrorist Attacks upon the United States, The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States (Washington, D.C.: 2004). The 9/11 Commission was an independent, bipartisan commission created in late 2002, to prepare a complete account of the circumstances surrounding the September 11, 2001 terrorist attacks, including preparedness for and the immediate response to the attacks. The Commission was also mandated to provide recommendations designed to guard against future attacks.

[10]In 2006, DHS reorganized their Information Analysis and Infrastructure Protection division. The functions of the Directorate of Information Analysis and Infrastructure Protection were moved to the Office of Intelligence Analysis and Office of Infrastructure Protection.

[11]HSPD-7 directed the DOT and DHS to collaborate on all matters relating to transportation security and transportation infrastructure protection. In 2003, DHS designated TSA as the lead agency for addressing HSPD-7 as it relates to securing the nation's transportation sector.

applying risk based principles. Our risk management framework entails a continuous process of managing risk through a series of actions, including setting strategic goals and objectives, assessing risk, evaluating alternatives, selecting initiatives to undertake, and implementing and monitoring those initiatives. DHS's NIPP describes a risk management process that closely mirrors our risk management framework.

Setting strategic goals, objectives, and constraints is a key first step in applying risk management principles and helps to ensure that management decisions are focused on achieving a purpose. These decisions should take place in the context of an agency's strategic plan that includes goals and objectives that are clear and concise. These goals and objectives should identify resource issues and external factors to achieving the goals. Further, the goals and objectives of an agency should link to a department's overall strategic plan. The ability to achieve strategic goals depends, in part, on how well an agency manages risk. The agency's strategic plan should address risk related issues that are central to the agency's overall mission.

Risk assessment, an important element of a risk based 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, vulnerability, and criticality or consequence. A threat assessment identifies and evaluates potential threats on the basis of factors such as capabilities, intentions, and past activities. A vulnerability assessment identifies weaknesses that may be exploited by identified threats and suggests options to address those weaknesses. 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. 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. The risk assessment element in the overall risk management cycle may be the largest change from standard management steps and can be important to informing the remaining steps of the cycle.

DHS Has Taken Steps to Assess Risk to Passenger Rail Systems, but Has Not Completed a Strategy for Securing the Transportation Sector

DHS has made progress in assessing the risks facing the U.S. passenger rail system, but has not completed a plan based on that risk assessment for securing the entire transportation sector and supporting plans for each mode of transportation, including passenger rail. The DHS OGT developed and implemented a risk assessment methodology to help passenger rail operators better respond to terrorist attacks and prioritize security measures. Passenger rail operators must have completed a risk assessment to be eligible for financial assistance through the fiscal year 2007 OGT Transit Security Grant Program, which includes funding for passenger rail. To receive grant funding, 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. As of February 2007, OGT had completed or planned to conduct risk assessments of most passenger rail operators. According to rail operators, OGT's risk assessment process enabled them to prioritize investments based on risk and allowed them to target and allocate resources towards security measures that will have the greatest impact on reducing risk across their rail systems.

Further, we reported in September 2005 that TSA had not completed a comprehensive risk assessment of the entire passenger rail system. TSA had begun to assess risks to the passenger rail system, including completing an overall threat assessment for both mass transit and passenger and freight rail modes. TSA also conducted criticality assessments of nearly 700 passenger rail stations and had begun conducting assessments for other passenger rail assets such as bridges and tunnels. TSA reported that it planned to rely on asset criticality rankings to prioritize which assets it would focus on in conducting vulnerability assessments to determine which passenger rail assets are vulnerable to attack. 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. We reported that, until all three assessments of passenger rail systems—threat, criticality, and vulnerability—have been completed, and until TSA determined how to use the results of these assessments to analyze and characterize the level of risk (high, medium, or low), it will be difficult to prioritize passenger rail assets and guide investment decisions about protecting them.

More recently, in January 2007, TSA reported taking additional actions to assess the risks facing the U.S. passenger rail system. For example, TSA reported that its surface transportation security inspectors are working with rail transit agencies to update risk assessments that FTA and FRA

conducted after September 11, and is also conducting additional security assessments of rail transit agencies. TSA also expected that the 50 largest rail transit agencies would complete security self assessments in early 2007. According to TSA, the agency is using the results of these assessments to set priorities and identify baseline security standards for the passenger rail industry. For example, the agency recently reported that it has identified underground and underwater rail infrastructure and high density passenger rail stations as the critical assets most at risk. According to TSA, the agency prioritized a list of the underwater rail tunnels deemed to be at highest risk, and plans to conduct assessments of high-risk rail tunnels.

We also reported in September 2005 that DHS was developing, but had not yet completed, a framework intended to help TSA, OGT, and other federal agencies work with their stakeholders to assess risk. This framework is intended to help the private sector and state and local governments 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 reported 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. We plan to assess DHS and DOT's progress in enhancing their risk assessment efforts during our follow-on review of passenger rail security.

Finalizing a methodology for assessing risk to passenger rail and other transportation modes and conducting risk assessments to determine the areas of greatest need are key steps required in developing a strategy for securing the overall transportation sector and each mode of transportation individually. However, TSA has not completed the required TSSP and supporting plans for securing each mode of transportation. According to TSA, the TSSP and supporting modal plans are in draft, but must be reviewed by DHS and the White House Homeland Security Council before they can be finalized. Until TSA issues the TSSP and modal plans, the agency lacks a clear strategy with goals and objectives for securing the overall transportation sector, including passenger rail.

Federal Agencies Have Taken Actions to Enhance Passenger Rail Security, Improve Federal Coordination, and Develop Industry Partnerships

In addition to ongoing initiatives to enhance passenger rail security conducted by the FTA and FRA before and after September 11, 2001, TSA issued security directives to passenger rail operators after the March 2004 terrorist attacks on the rail system in Madrid. However, federal and rail industry stakeholders have questioned the extent that these directives were based on industry best practices and expressed confusion about how TSA would monitor compliance with the directives. Since the completion of our work on passenger rail security, TSA has reported taking additional actions to strengthen the security of the passenger rail system. For example, TSA tested rail security technologies, developed training tools for rail workers, and issued a proposed rule in December 2006 regarding passenger and freight rail security, among other efforts. TSA has also taken steps to better coordinate with DOT regarding rail security roles and responsibilities and has worked to develop more effective partnerships with industry stakeholders. The memorandum of understanding between DHS and DOT was updated to include specific agreements between TSA and FTA in September 2005 and between TSA and FRA in September 2006 to delineate security-related roles and responsibilities, among other things, for passenger rail and mass transit. In addition, TSA established an Office of Transportation Sector Network Management and offices for each mode of transportation to develop security policies and partnerships with industry stakeholders, including passenger rail and other surface modes.

DOT Agencies Led Initial Efforts to Enhance Passenger Rail Security

Prior to the creation of TSA in November 2001, FTA and FRA, within DOT, 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 the September 11th attacks that are still in place today. Specifically, FTA launched a transit security initiative in 2002 that included security readiness assessments, technical assistance, grants for emergency response drills, and training. FTA also instituted the Transit Watch campaign in 2003—a nationwide safety and security awareness program designed to encourage the 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 OGT, and offer additional security awareness materials that address unattended bags and emergency evacuation procedures for transit agencies. In addition, in November 2003, FTA issued its Top 20 Security Program Action Items for Transit Agencies, which recommended measures for passenger rail operators to include 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. Further, in November 2004, FTA provided rail operators with security considerations for transportation infrastructure. This guidance provides 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, 2001. 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. In the wake of the Madrid terrorist bombings in March 2004, nearly 200 FRA inspectors, in cooperation with TSA, conducted 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 FTA and FRA 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 strengthen 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 Rail Security Directives, but Faces Challenges Related to Compliance and Enforcement

In May 2004, TSA issued security directives to the passenger rail industry to establish standard security measures for all passenger rail operators, including Amtrak.[12] However, as we previously reported, it was unclear how TSA developed the requirements in the directives, how TSA planned to monitor and ensure compliance, how rail operators were to implement the measures, and which entities were responsible for their implementation. According to TSA, the directives were based upon FTA and American Public Transportation Association 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.

[12]TSA issues security related regulations and directives pursuant to its 49 U.S.C. § 114(1) rulemaking authority.

While some of the directives' requirements correlate to information contained in the FTA guidance, the source for many of the requirements is unclear. Amtrak and FRA officials also raised concerns about some of the directives. For example, FRA officials stated that current FRA safety regulations requiring engineer compartment doors be kept unlocked to facilitate emergency escapes[13] conflicts with the TSA security directive requirement that doors equipped with locking mechanisms be kept locked. Other passenger rail operators we spoke with during our review stated that TSA did not adequately consult with the rail industry prior to developing and issuing these directives. In January 2007, TSA stated that it recognizes the need to closely partner with the passenger rail industry to develop security standards and directives.

As we reported in September 2005, rail operators are required to allow TSA and DHS to perform inspections, evaluations, or tests based on execution of the directives at any time or location. However, we reported that some passenger rail operators have expressed confusion and concern about the role of TSA's inspectors and the potential that TSA inspections could be duplicative of other federal and state rail inspections, such as FRA inspections. Since we issued our report, TSA officials reported that the agency has hired 100 surface transportation inspectors, whose stated mission is to, among other duties, monitor and enforce compliance with TSA's rail security directives. Further, in September 2006, FRA's and TSA's roles and responsibilities for compliance inspections were outlined in an annex to the existing memorandum of understanding between DHS and DOT. The annex provides that when an FRA inspector observes a security issue during an inspection, this information will be provided to TSA. Similarly, if a TSA inspector observes a safety issue, this information will be provided to FRA. According to TSA, since the initial deployment of surface inspectors, these inspectors have developed relationships with security officials in passenger rail and transit systems, coordinated access to operations centers, participated in emergency exercises, and provided assistance in enhancing security. We will continue to assess TSA's efforts to enforce compliance with rail security requirements, such as those included in the December 2006 proposed rule on rail security, during our follow-on review of passenger rail security that has been requested by your Committee Chairman.

[13]See 49 C.F.R. § 238.235.

TSA Has Reported Taking Additional Actions to Strengthen Passenger Rail Security, Improve Coordination with DOT, and Develop Industry Partnerships

In January 2007, TSA identified additional actions they had taken to strengthen passenger rail security. We have not verified or evaluated these actions. These actions include:

National explosive canine detection teams: Since late 2005, TSA reported that it has trained and deployed 53 canine teams to 13 mass transit systems to help detect explosives in the passenger rail system and serve as a deterrent to potential terrorists.

Visible Intermodal Prevention and Response Teams: This program is intended to provide teams of law enforcement, canines, and inspection personnel to mass transit and passenger rail systems to deter and detect potential terrorist actions. Since the program's inception in December 2005, TSA reported conducting more than 25 exercises at mass transit and passenger rail systems throughout the nation.

Mass Transit and Passenger Rail Security Information Sharing Network: According to TSA, the agency initiated this program in August 2005 to develop information sharing and dissemination processes regarding passenger rail and mass transit security across the federal government, state and local governments, and rail operators.

National Transit Resource Center: TSA officials stated that they are working with FTA and DHS OGT to develop this center, which will provide transit agencies nationwide with pertinent information related to transit security, including recent suspicious activities, promising security practices, new security technologies, and other information.

National Security Awareness Training Program for Railroad Employees: TSA officials stated that the agency has contracted to develop and distribute computer based training for passenger rail, rail transit, and freight rail employees. The training will include information on identifying security threats, observing and reporting suspicious activities and objects, mitigating security incidents, and other related information. According to TSA, the training will be distributed to all passenger and freight rail systems.

Transit Terrorist Tool and Tactics: This training course is funded through the Transit Security Grant Program and teaches transit employees how to prevent and respond to a chemical, biological, radiological, nuclear, or explosive attack. According to TSA, this course was offered for the first time during the fall of 2006.

National Tunnel Security Initiative: This DHS and DOT initiative aims to identify and assess risks to underwater tunnels, prioritize security funding to the most critical areas, and develop technologies to better secure underwater tunnels. According to TSA, this initiative has identified a list of 29 critical underwater rail transit tunnels.

DHS and TSA have also sought to enhance passenger rail security by conducting research on technologies related to screening passengers and checked baggage in the passenger rail environment. For example, TSA conducted a Transit and Rail Inspection Pilot, a $1.5 million effort to test the feasibility of using existing and emerging technologies to screen passengers, carry-on items, checked baggage, cargo, and parcels for explosives. According to TSA, the agency completed this pilot in July 2004. TSA officials told us that based upon preliminary analyses, the screening technologies and processes tested would be very difficult to implement on heavily used passenger rail systems because these systems carry high volumes of passengers and have multiple points of entry. However, TSA officials added that the screening processes used in the pilot may be useful on certain long-distance intercity train routes, which make fewer stops. Further, TSA 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 the pilot was used by TSA to screen certain passengers and belongings in Boston and New York rail stations during the 2004 Democratic and Republican national conventions. According to TSA, the agency is also researching and developing other passenger rail security technologies, including closed circuit television systems that can detect suspicious behavior, mobile passenger screening checkpoints to be used at rail stations, bomb resistant trash cans, and explosive detection equipment for use in the rail environment. Finally, TSA recently reported that the DHS Science and Technology (S&T) Directorate conducted a rail security pilot, which tested the effectiveness of explosive detection technologies in partnership with the Port Authority of New York and New Jersey.

In December 2006, TSA issued a proposed rule regarding passenger and freight rail security requirements. TSA's proposed rule would require that passenger and freight rail operators, certain facilities that ship or receive hazardous materials by rail, and rail transit systems take the following actions:

- Designate a rail security coordinator to be available to TSA on a 24 hour, seven day a week basis to serve as the primary contact for the receipt of intelligence and other security related information.
- Immediately report incidents, potential threats, and security concerns to TSA.
- Allow TSA and DHS officials to enter and conduct inspections, test, and perform other duties within their rail systems.
- Provide TSA, upon request, with the location and shipping information of rail cars that contain a specific category and quantity of hazardous materials within one hour of receiving the request from TSA.
- Provide for a secure chain of custody and control of rail cars containing a specified quantity and type of hazardous material.

The period for public comment on the proposed rule is scheduled to close in February 2007. TSA plans to review these comments and issue a final rule in the future.

With multiple DHS and DOT stakeholders involved in securing the U.S. passenger rail system and inherent relationships between security and safety, the need to improve coordination between the two agencies has been a consistent theme in our prior work in this area. In response to a previous recommendation we made,[14] 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. TSA signed annexes to the MOU with FRA in September 2006 and FTA in September 2005 describing the roles and responsibilities of each agency regarding passenger rail security. These annexes also describe how TSA and these DOT agencies will coordinate security related efforts, avoid duplicating

[14] *Transportation Security: Federal Action Needed to Help Address Security Challenges*, GAO-03-843 (Washington, D.C.: June 2003).

efforts, and improve coordination and communication with industry stakeholders.

In addition to the federal government, public and private rail operators share responsibility for securing passenger rail systems. As such, the need for TSA and other federal agencies to develop partnerships and coordinate their efforts with these operators is critical. To better coordinate and develop partnerships with industry stakeholders, TSA has established an Office of Transportation Sector Network Management (TSNM), which includes offices for each mode of transportation, such as mass transit (includes passenger rail), highways, including commercial vehicles, and pipelines. According to TSA, the TSNM Mass Transit Division coordinates federal security activities in the mass transit and passenger rail modes and works to develop partnerships with passenger rail operators, federal agencies, and industry associations. TSA also reports that it is working with industry partners to develop baseline security standards for passenger rail and other surface modes. We will continue to assess TSA's efforts in strengthening federal and private sector partnerships during our follow-on work on passenger rail security.

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, 2001, 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 tracks, 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 were not utilized, at the time of our review, by domestic rail operators or the U.S. government.

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. 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 attempted to enhance customer awareness. For example, 11 of the 13 operators we interviewed had implemented a customer awareness program.

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 11th, to provide security throughout their system or had taken steps to increase the visibility of their security personnel. 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 were more visible to customers and potential terrorists or criminals. Operators believed that these policies made it easier for customers to contact security personnel in the event of an emergency, or if they 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 were using canines to patrol their facilities or trains. Often, these units are used to detect the presence of explosives, and may be called in when a suspicious package is detected. 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 use 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.

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. Abroad, we found that 4 of 13 operators we interviewed had implemented forms of behavioral screening. 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 other reasons.

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 closed circuit television (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 that would be required, many rail operators felt that the cameras acted as a deterrent, assisted security personnel in determining how to respond to incidents that had already occurred, and could be monitored if an operator had received information that an incident may occur at a certain time or place in their system. Abroad, all 13 of the foreign rail operators we visited had CCTV systems in place. 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. 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.

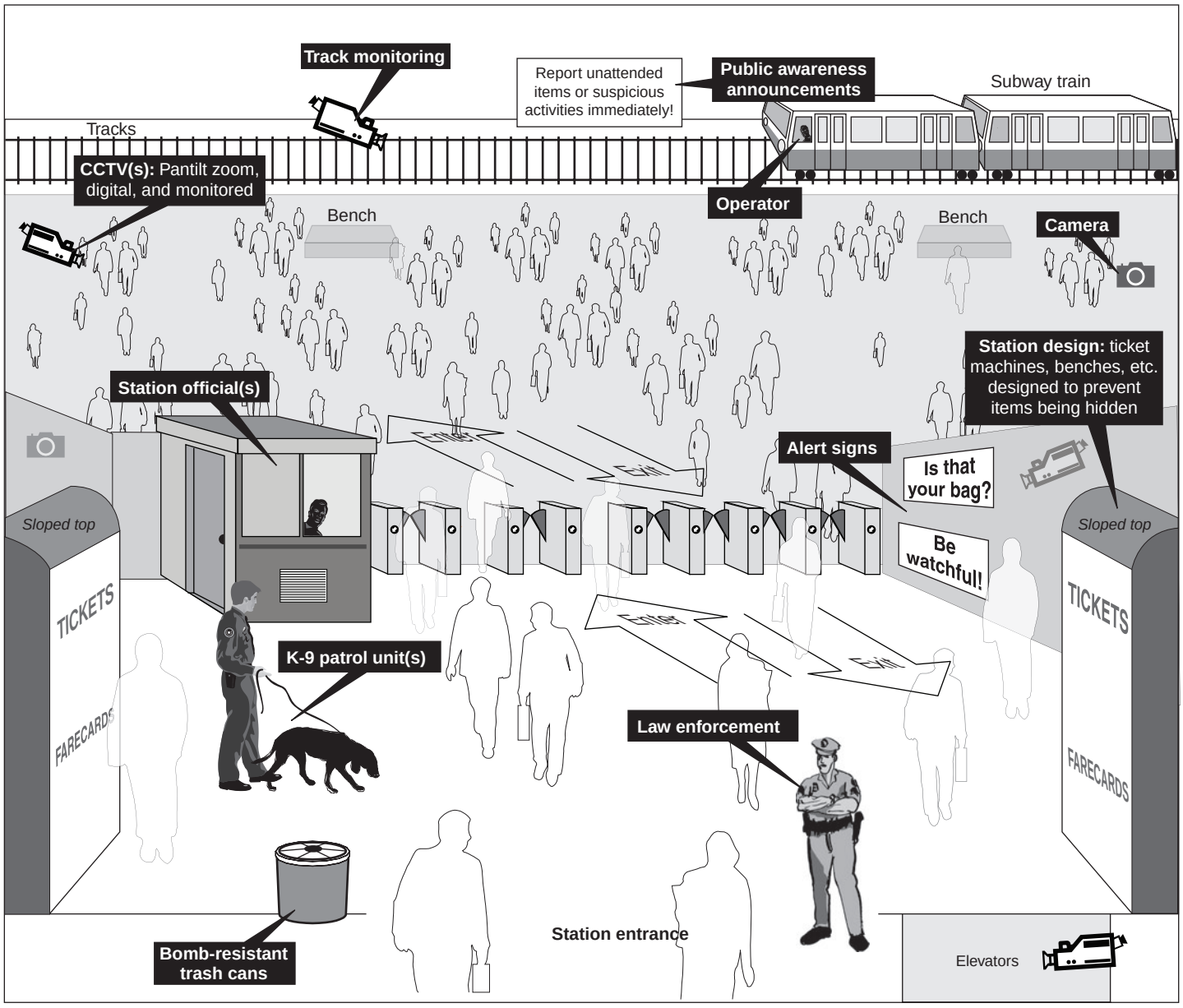
Access control: Tightening access control procedures at key facilities or rights-of-way is another way many rail operators have attempted to enhance security. A majority of domestic and selected foreign passenger rail operators had invested in enhanced systems to control unauthorized access at employee facilities and stations. Specifically, 23 of the 32 U.S. operators had installed a form of access control at key facilities and stations. All 13 foreign operators had implemented some form of access control to their critical facilities or rights-of-way.

Rail system design and configuration: In an effort to reduce vulnerabilities to terrorist attack and increase 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 also 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 had attempted to design new facilities with security in mind and had retrofitted older facilities to incorporate security-related modifications. For example, one foreign operator we visited was retrofitting its train cars with windows that passengers could open in the event of a chemical attack. In addition, the London Underground incorporates security into the design of all its new stations as well as when existing stations are modified. We observed several security features in the design of Underground stations, such as using vending machines that have no holes that someone could use to hide a bomb, and sloped tops to reduce the likelihood that a bomb can be placed on top of the machine. In addition, stations are designed to provide staff with clear lines of sight to all areas of the station, such as underneath benches or ticket machines, and station designers try to eliminate or restrict access to any recessed areas where a bomb could be hidden.

Figure 1 shows a diagram of several security measures that we observed in passenger rail stations both in the United States and abroad.

Figure 1: Composite of Selected Security Practices in the Passenger Rail Environment



Source: GAO and NOVA Development Corporation.

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

In our past work, we found that Amtrak faces security challenges unique to intercity passenger rail systems. First, Amtrak operates over thousands of miles, often far from large population centers. This makes its route system 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 and in stations owned by freight rail companies. This means that Amtrak often cannot 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. Finally, Amtrak's financial condition has never been strong—Amtrak has been on the edge of bankruptcy several times.

We reported in September 2005 that Amtrak had taken some actions to enhance security throughout its intercity passenger rail system. For example, Amtrak initiated a passenger awareness campaign, began enforcing restrictions on carry-on luggage that limit passengers to two carry-on bags, not exceeding 50 pounds; began requiring passengers to show identification after boarding trains; increased the number of canine units patrolling its system looking for explosives or narcotics; and assigned some of its police to ride trains in the Northeast Corridor. Also, Amtrak instituted a policy of randomly inspecting checked baggage on its trains. Amtrak was also 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. More recently, in January 2007, FRA reported that a systematic review of Amtrak's security policies and programs had been completed. According to FRA, the agency is currently working with Amtrak to implement the recommendations of this review.

Three Foreign Rail Security Practices Were Not 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 identified three foreign practices that were not currently in use among the U.S. passenger rail operators we contacted as of September 2005, nor were they performed by the U.S. government. These practices are as follows.

Covert testing: Two of the 13 foreign rail systems we visited utilized 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. TSA conducts covert testing of passenger and baggage screening in aviation, but has not conducted such testing in the rail environment.

Random screening: Of the 13 foreign operators we interviewed, 2 have some form of random screening of passengers and their baggage in place. Prior to the July 2005 London bombings, no passenger rail operators in the United States were practicing random passengers or baggage screening. However, during the Democratic National Convention in 2004, the Massachusetts Bay Transportation Authority instituted a system of random screening of passengers.

National government clearinghouse on technologies and best practices: According to passenger rail operators in five countries we visited, their national governments had centralized the process for performing research and development of passenger rail security technologies and maintained a clearinghouse of technologies and security best practices for passenger rail operators. We reported in September 2005 that no U.S. federal agency had compiled or disseminated information on research and development and other best practices for U.S. rail operators.

Implementing covert testing, random screening, or a government-sponsored clearinghouse for technologies and best practices in the U.S. could pose political, legal, fiscal, and cultural challenges because of the differences between the U.S. and these foreign nations. Many foreign nations have dealt with terrorist attacks on their public transportation systems for decades, compared with the United States, where rail has not been specifically targeted by terrorists. 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 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 rail 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 may be more willing to accept intrusive security measures. Nevertheless, in order to identify innovative security measures that could help further mitigate terrorism-risks to rail assets—especially as part of a broader risk management approach discussed earlier—it is important to consider the feasibility and costs and benefits of implementing the three rail security practices we identified in foreign countries. Officials from DHS, DOT, passenger rail industry associations, and rail systems we interviewed told us that operators would benefit from such an evaluation. Since our report on passenger rail security was issued, TSA has reported taking steps to coordinate with foreign passenger rail operators and governments to identify security best practices. For example, TSA reported working with British rail security officials to identify best practices for detecting and handling suspicious packages in rail systems. In addition, in January 2007, a TSA official stated that the agency was developing a clearinghouse of transportation security technologies, but a completion date for this effort was not currently available.

Conclusions

In conclusion, Madam Chairwoman, the 2005 London rail bombings and the 2006 rail attacks in Mumbai, India highlight the inherent vulnerability of passenger rail and other surface transportation systems to terrorist attack. Moreover, securing rail and other surface transportation systems is a daunting task, requiring that the federal government develop clear strategies that are based on an assessment of the risks to the security of the systems, including goals and objectives, for strengthening the security of these systems. Since our September 2005 report, DHS components have taken steps to assess the risks to the passenger rail system, such as working with rail operators to update prior risk assessments and facilitating rail operator security self assessments. According to TSA, the agency plans to use these assessment results to set priorities for securing rail assets deemed most at risk, such as underground and underwater rail infrastructure and high density passenger rail stations. A comprehensive assessment of the risks facing the transportation sector and each mode, including passenger rail, will be a key component of the TSSP and supporting plans for each mode of transportation. Until TSA completes these plans, however, the agency lacks a strategy with goals and objectives for securing the overall transportation sector and each mode of transportation, including passenger rail. TSA has also taken steps improve coordination with federal, state, and local governments, and has reported taking steps to strengthen partnerships with passenger rail industry stakeholders to enhance the security of the passenger rail system. As TSA moves forward to complete the TSSP and supporting plans for each mode

of transportation, it will be important that the agency articulate its strategy for securing rail and other modes to those government agencies and industry stakeholders that share the responsibility for securing these systems. We will continue to assess DHS and DOT's efforts to secure the U.S. passenger rail system during follow-on work to be initiated later this year.

Madam Chairwoman, 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. Individuals making key contributions to this testimony include John Hansen, Assistant Director, Chris Currie, and Tom Lombardi.

Related GAO Products Released Since September 11, 2001

Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts. GAO-07-225T. Washington, D.C.: January 18, 2007.

Passenger Rail Security: Evaluating Foreign Security Practices and Risk Can Help Guide Security Efforts. GAO-06-557T. Washington, D.C.: March 29, 2006.

Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts. GAO-06-181T. Washington, D.C.: October 20, 2005.

Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts. GAO-05-851. Washington, D.C.: September 9 2005.

Transportation Security: Systematic Planning Needed to Optimize Resources. GAO-05-357T. Washington, D.C.: February 15, 2005.

Rail Security: Some Actions Taken to Enhance Passenger and Freight Rail Security, but Significant Challenges Remain. GAO-04-598T. Washington, D.C.: March 23, 2004.

Transportation Security: Federal Action Needed to Enhance Security Efforts. GAO-03-1154T. Washington, D.C.: September 9, 2003.

Transportation Security: Federal Action Needed to Help Address Security Challenges. GAO-03-843. Washington, D.C.: June 30, 2003.

Rail Safety and Security: Some Actions Already Taken to Enhance Rail Security, but Risk-based Plan Needed. GAO-03-435. Washington, D.C.: April 30, 2003.

Transportation Security: Post-September 11th Initiatives and Long-term Challenges. GAO-03-616T. Washington, D.C.: April 1, 2003.

Mass Transit: Federal Action Could Help Transit Agencies Address Security Challenges. GAO-03-263. Washington, D.C.: December 13, 2002.

Mass Transit: Challenges in Securing Transit Systems. GAO-02-1075T. Washington, D.C.: September 18, 2002.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Mail or Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Congressional Relations

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

Public Affairs

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