

GAO

Testimony before Congressional
Subcommittees

For Release on Delivery
Expected at 10:00 a.m. EST
Wednesday, March 7, 2007

PASSENGER RAIL
SECURITY

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

Statement of Norman J. Rabkin, Managing Director
Homeland Security and Justice Issues





G A O

Accountability • Integrity • Reliability

Highlights

Highlights of GAO-07-583T, a testimony before Congressional Subcommittees

Why GAO Did This Study

The four rail attacks in Europe and Asia since 2004, including the most recent in India, highlight the vulnerability of passenger rail and other surface transportation systems to terrorist attack and demonstrate 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 recent program updates. Specifically, it addresses (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 assessments for securing all modes of transportation, including passenger rail, and (2) the actions that federal agencies have taken to enhance the security of the U.S. passenger rail system.

What GAO Recommends

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

www.gao.gov/cgi-bin/getrpt?GAO-07-583T

To view the full product, including the scope and methodology, click on the link above. For more information, contact Norman J. Rabkin at (202) 512-8777 or rabkinn@gao.gov.

PASSENGER RAIL SECURITY

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

What GAO Found

The DHS Office of Grants and Training (OGT) and TSA have begun to assess the risks facing the U.S. passenger rail system. However, GAO reported in September 2005 that TSA had not completed a comprehensive risk assessment of passenger rail. GAO found that, until TSA does so, it may be limited in its ability to prioritize passenger rail assets and help guide security investments. GAO 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 critical sectors. Since that time, TSA has reported taking additional steps to assess the risks to the passenger rail system. However, as of March 2, 2007, TSA has not issued the required Transportation Sector Specific Plan and supporting plans for passenger rail and other surface transportation modes, based on risk assessments. Until TSA does so, it lacks a clearly communicated strategy with goals and objectives for securing the 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, 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. OGT has also acted to help improve passenger rail security by, for example, providing funding for security enhancements to rail transit agencies and Amtrak through various grant programs. DHS and DOT have taken steps to better coordinate their respective rail security roles and responsibilities. In particular, DHS and DOT updated their memorandum of understanding to clarify their respective security roles and responsibilities for passenger rail.

Mr. Chairman, Madam Chairwoman, and Members of the Subcommittees:

Thank you for inviting me to participate in today's hearing on transit and rail security to discuss our recent work, primarily related to passenger rail security. Since its creation following the events of September 11, 2001, the Transportation Security Administration (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. Passenger rail systems, which include rail transit (commuter, heavy, and light rail) and intercity passenger rail, 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 four attacks in Europe and Asia since 2004, including the most recent in India, highlight the vulnerabilities of passenger rail systems and make clear that even when security precautions are put in place, these systems remain vulnerable to attack. Securing rail and surface transportation systems is a daunting task, requiring that the federal government develop a clearly communicated 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 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 passenger rail can sometimes lead to communication challenges, duplication of effort, and confusion about roles and responsibilities. Key Department of Homeland Security (DHS) stakeholders with critical roles include TSA, which is responsible for the security of all modes of transportation. In addition, the DHS Office of 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 rail safety and security. In addition, public and private passenger rail operators are responsible for securing their rail systems.

At the federal level, another challenge related to securing passenger rail systems involves allocating limited resources on the basis of 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 three key elements of risk—threat, vulnerability, and criticality or consequence—evaluating alternative security measures, selecting which measures to undertake, and implementing and monitoring those measures.

My testimony today focuses on the actions federal agencies have taken in developing and implementing security strategies and setting security priorities. In particular, my testimony highlights two 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 assessments for securing all modes of transportation, including passenger rail and (2) the actions that federal agencies have taken to enhance the security of the U.S. passenger rail system. My comments today are primarily based on our 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 United States, and 13

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

passenger rail operators in seven European and Asian countries.² In addition, we recently obtained selected updates from DHS on its efforts to secure passenger rail systems. We conducted our work in accordance with generally accepted government auditing standards.

In Summary

DHS has made progress in assessing the risks facing the U.S. passenger rail system, but has not issued a plan based on those risk assessments for securing the entire transportation sector and supporting plans for each mode of surface transportation, as required by and in accordance with the National Infrastructure Protection Plan. The DHS OGT has developed and conducted risk assessments of passenger rail systems to identify rail assets that are vulnerable to attack, such as stations and bridges. TSA has also conducted a threat assessment of mass transit and passenger rail and has identified critical rail assets. However, we reported in September 2005 that TSA had not completed a comprehensive risk assessment of the passenger rail system. We concluded that, until TSA completed this effort, it is 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 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. As part of that framework, TSA is developing, but 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 these plans, it lacks a clearly communicated strategy with goals and objectives for securing the overall transportation sector, including passenger rail.

²We have been requested to conduct a follow-on review of passenger rail security and to review the security of other surface modes of transportation—including freight rail, commercial vehicles, and highway infrastructure. We expect to have all this work underway this year.

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 implementing 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. Since we completed our work, TSA has taken 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 on passenger and freight rail security, among other efforts. DHS and DOT have also taken steps to better coordinate on rail security roles and responsibilities. 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.

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 March 2, 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).³ 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 fiscal year 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

³The American Public Transportation Association compiled these 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.

result in long lines that disrupt scheduled service. In addition, multiple 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 11 attacks, the role of federal agencies in securing the nation's transportation systems, including passenger rail, have continued to evolve. Prior to September 11, FTA and FRA, within DOT, were the primary federal entities 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 the security of all modes of transportation. Although its provisions focus primarily on aviation security, the act 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 DHS.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 (TSSP). 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 the sector, identify the critical assets and

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

⁵Pub. L. No. 108-458, §4001, 118 Stat. 3638, 3710-12 (codified at 49 U.S.C. § 114(t), 44904(c)-(d)).

⁶On 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).

infrastructure and develop programs to protect them, and develop security partnerships with industry stakeholders within the sector. As of March 2, 2007, TSA had not yet issued 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.

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

⁷OGT 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 and Preparedness (SLGCP). SLGCP was created to provide a "one-stop shop" for the numerous federal preparedness initiatives applicable to state and local governments. In 2005, SLGCP was incorporated under the Preparedness Directorate as OGT. Pursuant to the Department of Homeland Security Appropriations 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).

⁸FRA 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.

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 effort.⁹ Further, the Secretary of DHS has made risk-based decision making a cornerstone of departmental policy. 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

⁹National 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.

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

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 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

¹¹HSPD-7 directed 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.

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 Issued 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 issued a plan based on those risk assessments 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 tool 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 on the basis of 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, in January 2007 the agency 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's 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 issued 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 clearly communicated strategy with goals and objectives for securing the overall transportation sector, including passenger rail.

Federal Agencies Have Taken Actions to Enhance Passenger Rail Security

In addition to ongoing initiatives to enhance passenger rail security conducted by 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 to which these directives were based on industry best practices and expressed confusion about how TSA would monitor compliance with the directives. Since we completed 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. OGT has also acted to help improve passenger rail security by, for example, providing funding for security enhancements to rail transit agencies and Amtrak through various grant programs. DHS and DOT have taken steps to better coordinate their rail security roles and responsibilities. In particular, 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.

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 11 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 in 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 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 the directives' 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. 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 escapes¹³ 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 before 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. 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

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

¹³See 49 C.F.R. § 238.235.

to assess TSA's efforts to enforce compliance with rail security requirements, including those in the December 2006 proposed rule on rail security, during our follow-on review of passenger rail security.

TSA Has Reported Taking Additional Actions to Strengthen Passenger Rail Security

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 law enforcement, canines, and inspection teams 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 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 on 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, 7-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 1 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 was scheduled to close in February 2007. TSA plans to review these comments and issue a final rule in the future.

OGT Has Used Various Grant Programs to Fund Passenger Rail Security Since 2003

OGT has used various programs to fund passenger rail security since 2003. Through the Urban Area Security Initiative (UASI) grant program, OGT has provided grants to urban areas to help enhance their overall security and preparedness level to prevent, respond to, and recover from acts of terrorism. In 2003 and 2004, \$65 million and \$50 million, respectively, were provided to rail transit agencies through the UASI program. In addition, the DHS Appropriations Act 2005 appropriated \$150 million for rail transit, intercity passenger rail, freight rail, and transit security grants.¹⁴ OGT used this funding to build on the work under way through the UASI program and create and administer new programs focused specifically on transportation security, including the Transit Security Grant Program and the Intercity Passenger Rail Security Grant Program. These programs provided 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

¹⁴Pub. L. No. 108-334, 118 Stat. 1298, 1309 (2004). The fiscal year 2006 DHS appropriations act also appropriated \$150 million and the fiscal year 2007 DHS appropriations act appropriated \$175 million for the same purpose. Pub. L. No. 109-90, 119 Stat. 2064, 2076 (2005); Pub. L. No. 109-295, 120 Stat. 1355, 1369 (2006).

through the Intercity Passenger Rail Security Grant Program. During fiscal year 2007, OGT plans to distribute \$156 million for rail and bus security grants and \$8 million to Amtrak.

In January 2007, OGT reported that the Intercity Passenger Rail Security Program had been incorporated into the Transit Security Grant Program. The President's fiscal year 2008 budget request includes \$175 million for the Transit Security Grant Program. According to budget documents, grants will be awarded to rail transit agencies and Amtrak for preparedness activities related to terrorism and other incidents on the basis of risk and effectiveness.¹⁵

Although OGT has distributed hundreds of millions of dollars in grants to improve passenger rail security, issues have surfaced about the grant process.

- **Changes to grant requirements:** As DHS works to refine its risk assessment methodologies, develop better means of assessing proposed investments using grant funds, and align grant guidance with the implementation of broader emergency preparedness goals, such as implementation of the National Preparedness Goal, it has annually made changes to the guidance for the various grants it administers. These changes include changes in the eligibility for grants. As a result of these annual changes, awardees and potential grant recipients must annually review and understand new information on the requirements for grant applications including justification of their proposed use of grant funds.
- **Allowable uses of grants:** Funds awarded through the Transit Security Grant Program can be used to supplement funds received from other grant programs. However, allowable uses are not clearly defined. For example, Transit Security Grant Program funds

¹⁵The Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users provided that DOT and DHS shall jointly issue final regulations to establish the characteristics of and requirements for public transportation security grants, including funding priorities, eligible activities, methods for awarding grants, and limitations on administrative expenses. See Pub. L. No. 109-59, § 3028(c), 119 Stat. 1144, 1624-25 (2005). According to language contained in the draft proposed rule, the rule will provide for interagency coordination between DHS and FTA with regard to the transit security grant program.



can be used to create canine teams but cannot be used to maintain these teams—that is, the grant funds cannot be used for food, medical care, and other such maintenance costs for the dogs on the team. Whether other grant funds could be used for such maintenance costs would be governed by the terms of those grants. Grant recipients have expressed a need for clear guidance on the allowable use of grants and how they can combine funds from more than one grant to fund and implement specific projects.

DHS and DOT Have Worked to Improve Coordination on Passenger Rail Security

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,¹⁶ DHS and DOT signed a memorandum of understanding (MOU) in September 2004 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 acknowledges that DHS has primary responsibility for transportation security, with DOT playing a supporting role by providing technical assistance and helping DHS implement security policies.

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.¹⁷ TSA signed annexes to the MOU with FRA in September 2006 and FTA in September 2005. These annexes describe each agency's roles and responsibilities for passenger rail security. These annexes also describe how TSA and these DOT agencies will coordinate security-related efforts, avoid duplication of efforts, and improve coordination and

¹⁶GAO, *Transportation Security: Federal Action Needed to Help Address Security Challenges*, GAO-03-843 (Washington, D.C.: June 2003).

¹⁷We did not examine the appropriateness or assess the efficiency of the how DHS and DOT have divided and assigned security-related roles in the MOU or annexes.

Table 1: Examples of Responsibilities Divided between DHS and DOT as Outlined in MOU Annexes

<p>Assessments and resulting measures</p>	<p>DHS is the lead agency responsible for assessing risk to passenger rail systems.</p> <p>DHS is to share risk assessment results with FTA to ensure FTA's training and technical assistance programs conform to DHS policy.</p> <p>TSA is to consult with FRA in the development of security procedures that impact rail facilities or operations and ensure they do not conflict with safety requirements.</p>	<p>FTA may review security-related issues on FTA-funded transit projects and is to invite DHS to participate.</p> <p>FTA is to share the results of the limited number of vulnerability assessments it conducts with DHS.</p> <p>FRA is to provide TSA with data from security inspections and other reviews.</p>
<p>Threat information</p>	<p>DHS is to communicate relevant intelligence information, including threats and warnings, and changes to the national threat condition to DOT and rail industry stakeholders in a timely manner.</p>	<p>DOT is to communicate relevant intelligence information, including threats and warnings, to DHS.</p>
<p>Protective measures</p>	<p>DHS is to consult with DOT before disseminating security requirements.</p>	<p>DOT is to consult with DHS before disseminating safety requirements, including safety measures with security implications.</p>
<p>Public awareness</p>	<p>DHS is to support FTA's security awareness program, Transit Watch, with available funds.</p>	<p>FTA is to implement and support Transit Watch and coordinate this program with DHS's Citizen Corps, a public participation program.</p>

agencies said they were unsure of lines of responsibility for transit security oversight and said they were confused about what standards they would be required to meet. For example, while state oversight agencies are free to create their own standards, TSA issued rail security directives in May 2004 and has authority to undertake regulatory actions that impose requirements upon transit agencies. To reduce confusion among transit and oversight agencies, we recommended last year that TSA 1) coordinate with FTA to clearly articulate to state oversight agencies and transit agencies the roles and responsibilities TSA develops for its rail inspectors, and 2) work with state oversight agencies to coordinate their security audits whenever possible and include FTA in this communication to help ensure effective coordination with these agencies. FTA and TSA officials stated that they are working to determine how to implement the recommendations.

Conclusions

In conclusion, the rail attacks in Europe and Asia 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 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 issues these plans, however, the agency lacks a clearly communicated strategy with goals and objectives for securing the overall transportation sector and each mode of transportation, including passenger rail. As TSA moves forward to issue 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.

With the execution of the MOU and related annexes, DHS and DOT have taken important steps forward in improving coordination among the

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