United States Government Accountability Office

GAO

Testimony before the Committee on Transportation and Infrastructure, Subcommittee on Highways, Transit, and Pipelines, House of Representatives

For Release on Delivery
Expected at 2:00 p.m. EST
Wednesday, March 29, 2006

PASSENGER RAIL SECURITY

Evaluating Foreign Security Practices and Risk Can Help Guide Security Efforts

Statement of JayEtta Z. Hecker, Director
Physical Infrastructure Issues

March 29, 2006

PASSENGER RAIL SECURITY

Evaluating Foreign Security Practices and Risk Can Help Guide Security Efforts

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-06-557T, a testimony before the Committee on Transportation and Infrastructure, Subcommittee on Highways, Transit, and Pipelines, House of Representatives

Why GAO Did This Study

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

This testimony, which is based primarily on GAO's September 2005 report on passenger rail security (GAO-05-851), provides information on (1) the security practices that domestic and selected foreign rail transit operators have implemented to mitigate risks and enhance security; (2) the Department of Homeland Security's (DHS) and the Department of Transportation's (DOT) funding of rail transit security and use of risk management in funding decisions; and (3) the steps DHS and DOT have taken to improve coordination on rail transit security matters. As part of its 2005 report, GAO contacted 32 U.S. rail transit operators and 13 passenger rail operators in seven European and Asian countries.

What GAO Recommends

GAO's September 2005 report on passenger rail security recommended, among other things, that the Secretary of Homeland Security, in collaboration with DOT, determine the feasibility of implementing certain rail security practices used in foreign countries. DHS and DOT generally agreed with the report's recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-06-557T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact JayEtta Z. Hecker at (202) 512-2834 or Cathleen A. Berrick (202) 512-3404.

What GAO Found

Domestic and foreign rail transit operators GAO contacted have taken similar actions to help secure their systems, including implementing customer awareness programs, increasing the number and visibility of their security personnel, and upgrading security technology. Also, both domestic and foreign operators have used risk assessments to guide security-related activities and spending. However, GAO also observed security practices that were used by certain foreign passenger rail operators, but were not employed in the United States at the time of GAO's review. For example, some foreign rail operators use covert testing to help keep employees alert to security threats or randomly screen passengers. Centralized clearinghouses on rail security technologies, such as chemical sensors, and best practices are also maintained in some foreign countries. While introducing any of these security practices into the U.S. rail system may pose political, legal, fiscal, and cultural challenges, the practices may nevertheless warrant further examination.

Both DHS and DOT help fund rail transit security investments, and DHS has promoted risk-based funding decisions in the allocation of transit security grants. DHS's Office of Grants and Training is the primary source of security funding for passenger rail systems, providing over $320 million in grants to rail transit agencies for fiscal years 2003 to 2006. The Office of Grants and Training has leveraged its grant-making authority to promote risk-based funding decisions for passenger rail by requiring, for example, that operators complete a risk assessment to be eligible for a transit security grant. As we have noted in previous reports, using assessments of risk to target resources to the highest priority is especially critical given the competition for resources within the rail transit sector, and between the rail transit sector and the other modes of transportation. DOT's Federal Transit Administration (FTA) also helps fund rail transit security efforts by providing financial assistance to transit agencies and requiring that they spend 1 percent of their urbanized area formula funds on security improvements.

To improve coordination on transportation security matters, including rail transit security, DHS and DOT signed a memorandum of understanding (MOU) in September 2004. DHS and DOT also signed a transit security annex to the MOU in September 2005 that delineates specific security-related roles, responsibilities, resources, and commitments for transit issues. In GAO's view, these actions are positive steps forward in addressing the coordination problems GAO previously identified. For instance, federal and rail industry officials raised questions about the feasibility of implementing and complying with TSA's May 2004 security directives, citing limited opportunities to collaborate with TSA to ensure that industry best practices were incorporated. Effective coordination between DHS and DOT will continue to be important as both departments move forward with existing programs and new security initiatives.

Mr. Chairman and Members of the Subcommittee:

Thank you for inviting me to participate in today's hearing on rail transit security. The London rail bombings that took place in July 2005—resulting in over 50 fatalities and more than 700 injuries—made clear that even when a variety of security precautions are in place, rail transit systems that move high volumes of passengers each day remain vulnerable to terrorist attack. While securing the U.S. rail transit system is a daunting task—a shared responsibility requiring coordinated action on the part of federal, state, and local governments and the private sector—it is important nonetheless to take the necessary steps to identify and mitigate risks to rail transit systems.

As we have reported previously, the sheer number of stakeholders involved in securing these systems can lead to communication challenges, duplication of effort, and confusion about roles and responsibilities. Key federal stakeholders with critical roles to play within the rail sector include the Transportation Security Administration (TSA), which is responsible for transportation security overall, and the Office of Grants and Training,[1] which provides grant funds to rail operators and conducts risk assessments for passenger rail agencies, both within the Department of Homeland Security (DHS); and the Federal Transit Administration (FTA) and Federal Railroad Administration (FRA), both within the Department of Transportation (DOT). One of the critical challenges facing these federal agencies, and the rail system operators they oversee or support, is finding ways to protect rail systems from potential terrorist attacks without compromising the accessibility and efficiency of rail transit.

At the federal level, another significant challenge to securing rail systems involves the allocation of resources. Rail transit systems represent one of many modes of transportation—along with aviation, maritime, and others—competing for limited federal security resources. Within the rail transit sector itself, there is competition for resources, as federal, state, and local agencies and rail operators seek to identify and invest in appropriate security measures to safeguard these systems while also investing in other capital and operational improvements. Moreover, given competing priorities and limited homeland security resources, difficult policy decisions have to be made by Congress and the executive branch to

[1]DHS's Office of Grants and Training was formerly called the Office of Domestic Preparedness.

prioritize security efforts and direct resources to the areas of greatest risk within the rail transit system, among all transportation modes, and across other nationally critical sectors.

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

My testimony will cover three areas: (1) the security practices that domestic and selected foreign rail transit operators have implemented to mitigate risks and enhance security, and any differences in these practices; (2) DHS's and DOT's funding of rail transit security and use of risk management in funding decisions; and (3) the steps DHS and DOT have taken to improve coordination on rail transit security matters. My comments today are based on our body of work on passenger rail security issues, including our September 2005 report to the Chairman of the House Transportation and Infrastructure's Subcommittee on Railroads, Senators Snowe and Boxer, and Representative Castle.[3] For this report, we

[2]Pub. L. No. 108-458, 118 Stat. 3638. For more information on risk management, see GAO, *Transportation Security: Systematic Planning Needed to Optimize Resources*, GAO-05-357T (Washington, D.C.: Feb. 15, 2005); *Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts*, GAO-02-208T (Washington, D.C.: Oct. 31, 2001); and *Combating Terrorism: Threat and Risk Assessments Can Help Prioritize and Target Program Investments*, GAO/NSIAD-98-74 (Washington, D.C.: Apr. 9, 1998).

[3]GAO, *Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts*, GAO-05-851 (Washington, D.C.: Sept. 9, 2005); GAO, *Rail Security: Some Actions Taken to Enhance Passenger and Freight Rail Security, but Significant Challenges Remain*, GAO-04-598T (Washington, D.C.: Mar. 24, 2004); GAO, T*ransportation Security: Federal Action Needed to Help Address Security Challenges*, GAO-03-843 (Washington, D.C.: June 30, 2003); and GAO, *Mass Transit: Federal Actions*

contacted 32 U.S. rail transit operators and 13 passenger rail operators in seven European and Asian countries. These domestic and foreign rail agencies and the areas they serve are listed in appendix I. All of the reports on which this statement is based were prepared in accordance with generally accepted government auditing standards.

In summary:

- Domestic and foreign rail transit operators we contacted have taken similar actions to help secure their systems, such as implementing customer awareness programs, upgrading security technology, and tightening access controls. Also, both domestic and foreign operators have used risk assessments to guide security-related activities and funding. However, we also observed rail security practices in foreign countries that were not in use domestically at the time of our review. For example, some foreign rail operators use covert testing to help keep employees alert to security threats or randomly screen passengers. In addition, centralized clearinghouses on rail security technologies, such as chemical sensors, and best practices are maintained in some foreign countries. While introducing any of these security practices into the U.S. rail system may pose political, legal, fiscal, and cultural challenges, the practices may nevertheless warrant further examination. In our September 2005 report on passenger rail security, we recommended, among other things, that the Secretary of Homeland Security, in collaboration with DOT and the passenger rail industry, determine the feasibility, in a risk management context, of implementing certain rail security practices used in foreign countries, including covert testing and random screening, an information clearinghouse for security technologies and best practices, and practices that integrate security into infrastructure design.[4] DHS and DOT generally agreed with the report's recommendations.

- Both DHS and DOT help fund rail transit security investments, and DHS has promoted risk-based funding decisions in the allocation of transit security grants. DHS's Office of Grants and Training is the primary source of security funding for passenger rail systems. From fiscal year 2003 through fiscal year 2006, the Office of Grants and Training provided over $320 million in grants to rail transit agencies

Could Help Transit Agencies Address Security Challenges, GAO-03-263 (Washington, D.C.: Dec. 13, 2002).

[4]GAO-05-851.

through the Urban Area Security Initiative (UASI) and the Transit Security Grant Programs. The Office of Grants and Training has leveraged its grant-making authority to promote risk-based funding decisions for passenger rail by requiring, for example, that operators complete a risk assessment to be eligible for a transit security grant. Using assessments of risk to target resources to the highest priority is especially critical given the competition for resources within the rail transit sector, and between the rail transit sector and the other modes of transportation. Moreover, as the 2005 London rail bombings dramatically illustrated, even when a variety of security precautions are put in place, passenger rail systems remain vulnerable and attractive targets given their open designs and the high volumes of passengers they transport each day. Thus, it is important that limited resources are targeted to security activities that have the greatest impact on reducing overall risk. DOT's FTA also helps fund rail transit security efforts through the financial assistance it provides to transit agencies. In addition, FTA requires that a certain percentage of federal funds be devoted to security activities. Specifically, transit agencies are required to spend 1 percent of their urbanized area formula funds on security improvements.[5]

- To improve coordination on transportation security matters, including rail transit security, DHS and DOT signed a memorandum of understanding (MOU) in September 2004. The MOU defines broad areas of responsibility for each department. The two departments also signed a transit security annex to the MOU in September 2005 that delineates the specific security-related roles, responsibilities, resources, and commitments for transit issues. We believe these actions are positive steps forward in addressing the coordination problems we have previously identified. For instance, in 2004, TSA issued emergency security directives to domestic rail operators after terrorist attacks on the rail system in Madrid. However, federal and rail industry officials raised questions about the feasibility of implementing and complying with these directives, citing limited opportunities to collaborate with TSA to ensure that industry best practices were incorporated. Effective coordination between DHS and DOT will continue to be important as both departments move forward with existing programs and new security initiatives. For example, to avoid

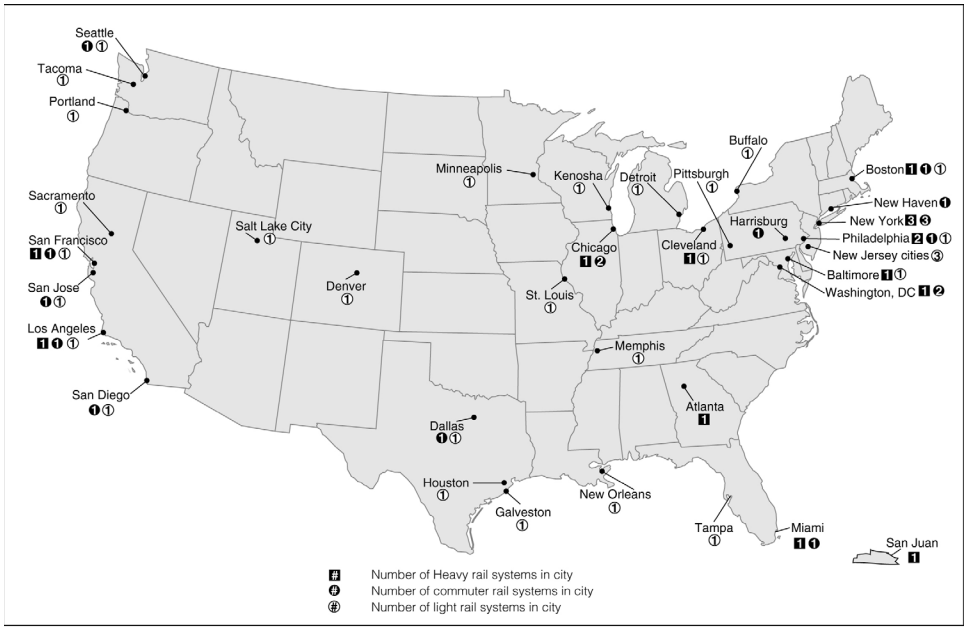
[5]FTA's urbanized area formula grant program provides federal funds to urbanized areas (jurisdictions with populations of 50,000 or more) for transit capital investments, operating expenses, and transportation-related planning.

duplication and confusion, it will be important that TSA coordinate the oversight activities of its rail inspectors with those of the state auditors from FTA's State Safety Oversight program and FRA's rail safety inspectors.

Background

Each weekday, 11.3 million passengers in 35 metropolitan areas and 22 states use some form of rail transit—that is, heavy, commuter, and light rail. Heavy rail systems—subway systems like New York City's transit system and Washington, D.C.'s Metro—typically operate on fixed rail lines within a metropolitan area and have the capacity for a heavy volume of traffic. Commuter rail systems generally operate on railroad tracks and provide regional service (e.g., between a central city and adjacent suburbs)—and are traditionally associated with older industrial cities, such as Boston, New York, and Chicago. Light rail systems are typically characterized by lightweight passenger rail cars that operate on track that is not separated from vehicular traffic for much of the way. Figure 1 identifies the geographic location of rail transit systems within the United States.

Figure 1: Geographic Distribution of Rail Transit Systems



Source: National Transit Database.

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

Securing the nation's rail transit systems is a shared responsibility requiring coordinated action on the part of federal, state, and local governments; the private sector; and the passengers who ride these rail systems. Since the September 11 attacks, the role of federal government agencies in securing the nation's transportation systems, including rail transit, have continued to evolve. Before September 11, DOT—namely, FTA—was the primary federal entity involved in rail transit security matters. In response to the attacks of September 11, Congress passed the Aviation and Transportation Security Act (ATSA), which created TSA within DOT and defined its primary responsibility as ensuring security in all modes of transportation.[6] The act also gave TSA regulatory authority for security over all transportation modes. ATSA does not specify TSA's roles and responsibilities in securing the maritime and land transportation modes at the level of detail it does for aviation security. Instead, the act broadly identifies TSA as responsible for ensuring the security of all modes of transportation. With the passage of the Homeland Security Act of 2002, TSA was transferred, along with over 20 other agencies, to DHS.[7] While TSA is the lead federal agency for ensuring the security of all transportation modes, FTA conducts nonregulatory safety and security activities, including safety- and security-related training, research, technical assistance, and demonstration projects. In addition, FTA promotes safety and security through its grant-making authority.

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

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

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

U.S. rail transit 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 system facilities, such as track, buildings, and train cars. All of the U.S. rail transit operators we contacted have implemented some security measures—such as customer awareness programs and more, and more visible, security personnel—that were generally consistent with those we observed in Europe and Asia. We also identified three rail security practices—covert testing, random screening of passengers and their baggage, and maintaining a centralized clearinghouse on rail security technologies—used in foreign countries but not, at the time or our review, domestically.[8]

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

Both U.S. and foreign rail transit operators we contacted have implemented similar improvements to enhance the security of their systems. To guide security actions and spending, domestic and foreign operators—even the privatized foreign systems—consider risk assessments, budget constraints, and other factors. For example, one foreign rail operator with a daily ridership of 2.3 million passengers used a risk management methodology to assess risks, threats, and vulnerabilities to rail in order to guide security spending. According to the operator, the methodology employs a "risk informed" approach to support management's business decision process regarding security. A summary of domestic and foreign security practices follows.

Customer awareness: Customer awareness programs we observed used signs and announcements to encourage riders to alert train staff if they observed suspicious packages, persons, or behavior. Of the 32 domestic rail operators we interviewed, 30 had implemented a customer awareness program or made enhancements to an existing program. Foreign rail operators we visited also attempt to enhance customer awareness. For example, 11 of the 13 operators we interviewed had implemented a customer awareness program. Similar to programs of U.S. operators, these programs used signs, announcements, and brochures to inform passengers

[8]At the time we completed our work in June 2005, these three practices were not utilized. However, as discussed later in this testimony, some rail operators began using random screening in the aftermath of the July bomb attacks on the London subway system and others may have begun utilizing this or other security practices since our report.

and employees about the need to remain vigilant and report any suspicious activities.

More, and more visible security personnel: Of the 32 U.S. rail operators we interviewed, 23 had increased the number of security personnel they used since September 11, to provide security throughout their system or had taken steps to increase the visibility of their security personnel. For example, several U.S. and foreign rail operators we spoke with had instituted policies such as requiring their security staff to wear brightly colored vests and patrol trains or stations more frequently, so they are more visible to customers and potential terrorists or criminals. These policies make it easier for customers to contact security personnel in the event of an emergency, or if they have spotted a suspicious item or person. At foreign sites we visited, 10 of the 13 operators had increased the number of their security officers throughout their systems in recent years because of the perceived increase in the risk of a terrorist attack.

Increased use of canine teams: Of the 32 U.S. rail transit operators we contacted, 21 had begun to use canine units, which include both dogs and human handlers, to patrol their facilities or trains or had increased their use of such teams. In foreign countries we visited, rail transit operators' use of canine units varied. In some Asian countries, dogs were not culturally accepted by the public and thus were not used for rail security purposes. Most European rail transit operators used canine units for explosives 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 to respond to events once they occur. For example, the London Underground and the British Transport Police developed the "HOT" method for Underground employees to identify suspicious items in the rail system. In the HOT method, employees are trained to look for packages or items that are Hidden, Obviously suspicious, and not Typical of the environment. If items meet all of these criteria, employees are to notify station managers, who are to call in the authorities and potentially shut down the station or take other action. According to London Underground officials, the HOT method has significantly reduced the number of system disruptions caused when a suspicious item was identified. Several rail transit operators in the United States and abroad have trained their employees in the HOT method. It is important to note that such training is

not designed to prevent acts of terrorism like the July 2005 London attacks, in which suicide bombers killed themselves rather than leaving bombs behind.

Passenger and baggage screening practices: Some domestic and foreign rail operators have trained employees to recognize suspicious behavior as a means of screening passengers. Eight U.S. rail transit operators we contacted were using some form of behavioral screening. For example, the Massachusetts Bay Transportation Authority (MBTA), which operates Boston's T system, has adopted a behavioral screening system to identify passengers exhibiting suspicious behavior. The Massachusetts State Police train all MBTA personnel to be on the lookout for behavior that may indicate someone has criminal intent, and to approach and search such persons and their baggage when appropriate. Abroad, we found that 4 of the 13 operators we interviewed had implemented forms of behavioral screening similar to MBTA's system. All of the domestic and foreign rail operators we contacted have ruled out an airport-style screening system for daily use in heavy traffic. According to the operators, such a system, in which each passenger and the passenger's baggage are screened by a magnetometer or X-ray machine, raised concerns about cost, staffing, and customer convenience, among other factors.

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 the operators said would be required, many rail operators told us the cameras act as a deterrent, assist security personnel in determining how to respond to incidents that have already occurred, and can be monitored if an operator has received information that an incident may occur at a certain time or place in a system. One rail operator, New Jersey Transit, had installed "smart" cameras, which were programmed to alert security personnel when suspicious activity occurred, such as if a passenger left a bag in a certain location or a boat docked under a bridge. According to the New Jersey Transit officials, this technology was relatively inexpensive and not difficult to implement. Several other operators said they were interested in exploring this technology. Abroad, all 13 of the foreign rail operators we visited had CCTV systems in place. As in the United States, foreign rail operators use these cameras primarily to deter crime and to respond to

incidents after they occur, because they do not have enough staff to monitor all the cameras continuously.

Most rail operators we spoke with had not installed equipment for detecting chemical or biological agents because of the costs involved, but a few operators had this equipment or were exploring its purchase. For example, the Washington Metropolitan Area Transit Authority (WMATA), in Washington, D.C., has installed these sensors in some of its stations, thanks to a program jointly sponsored by DOT and the Department of Energy that provided this equipment to WMATA because of the high perceived likelihood of an attack in Washington, D.C. Also, at the time of our review, at least three other domestic rail operators we spoke with were exploring the possibility of partnering with federal agencies to install such equipment in their facilities on an experimental basis. Also, as in the United States, a few foreign operators had implemented chemical or biological detection devices at rail stations, but their use was not widespread. Two of the 13 foreign operators we interviewed had implemented these sensors, and both were doing so on an experimental basis. In addition, police officers from the British Transport Police—responsible for policing the rail system in the United Kingdom—were equipped with pagers to detect chemical, biological, or radiological elements in the air, allowing them to respond quickly in case of a terrorist attack using one of these methods. The British Transit Police also have three vehicles carrying devices to determine if unattended baggage contains explosives. These vehicles patrol the system 24 hours per day.

Access control: Tightening access procedures at key facilities or rights-of-way is another way many rail operators have attempted to enhance security. A majority of domestic and selected foreign passenger rail operators had invested in enhanced systems to control unauthorized access at employee facilities and stations. Specifically, 23 of the 32 U.S. operators had installed a form of access control at key facilities and stations. This often involved installing a system requiring employees to swipe an access card to gain access to control rooms, repair facilities, and other key locations. All 13 foreign operators had implemented some system to control access to their critical facilities or rights-of-way.

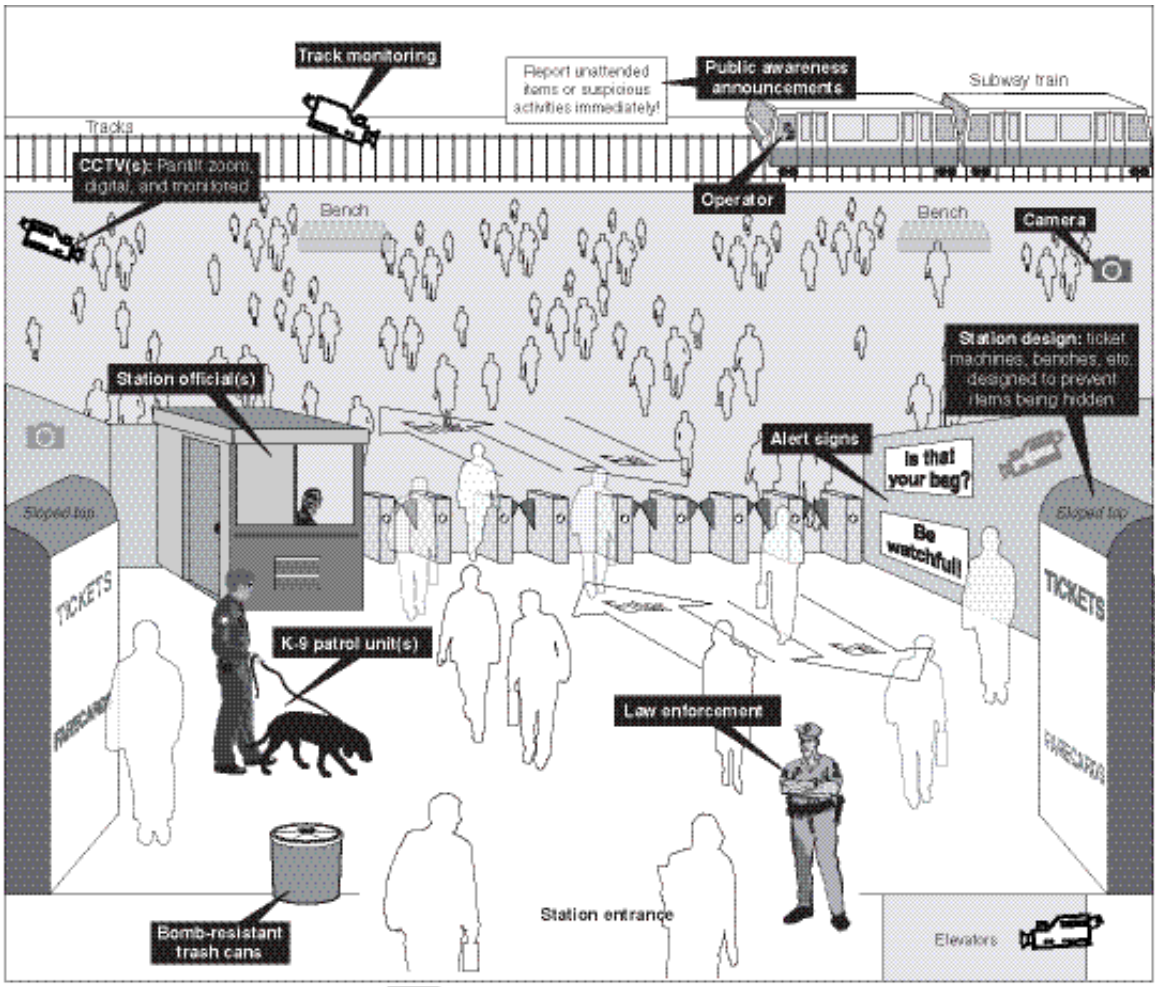
Rail system design and configuration: In an effort to reduce vulnerabilities to terrorist attack and increase overall security, rail transit operators in the United States and abroad have been, or are now beginning to, incorporate security features into the design of new and existing rail infrastructure, primarily rail stations. For example, of the 32 domestic rail

operators we contacted, 22 had removed their conventional trash bins entirely, or replaced them with transparent or bomb-resistant trash bins, as TSA directed in May 2004. Foreign rail operators had taken steps to remove traditional trash bins from their systems. Of the 13 operators we visited, 8 had either removed their trash bins entirely or replaced them with blast-resistant cans or transparent receptacles.

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

In the United States, several rail transit operators said they were taking security into account when designing new facilities or remodeling older ones. Twenty-two of 32 rail operators we interviewed told us that they were incorporating security into the design of new or existing rail infrastructure. For example, New York City Transit and Port Authority Trans-Hudson (PATH) officials told us they are incorporating security into the design of its new stations, including the redesigned Fulton Street station and the World Trade Center Hub that were damaged or destroyed during the September 11 attacks. In addition, in June 2005, FTA issued guidelines for use by the transit industry encouraging the incorporation of particular security features into the design of transit infrastructure. These guidelines include, for example, increasing visibility for onboard staff, reducing the areas where someone could hide an explosive device on a transit vehicle, and enhancing emergency exits in transit stations. Figure 2 illustrates several security measures that we observed in rail transit stations both in the United States and abroad. It should be noted that this figure represents an amalgam of stations we visited, not any particular station.

Figure 2: Composite of Selected Security Practices in the Rail Transit Environment



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

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

Covert testing: Two of the 13 foreign rail systems we visited use 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 alarms. In one European system, security staff place suspicious items throughout their system to see how long it takes operating staff to respond to the items. Similarly, one Asian rail operator's security staff break security seals on fire extinguishers and open alarmed emergency doors randomly to see how long it takes staff to respond. Officials of these operators stated that these tests are carried out daily and are beneficial because the staff know they could be tested at any moment and are therefore more likely to be vigilant about security.

Random screening: Of the 13 foreign operators we interviewed, 2 conducts some form of random screening of passengers and their baggage. In the systems where this practice is used, security personnel can approach passengers either in stations or on the trains and ask them to submit their persons or their baggage to a search. Passengers declining to cooperate must leave the system. For example, in Singapore, rail agency officials rotate the stations where they conduct random searches so that the searches are carried out at a different station each day. Before the July 2005 London bombings, no rail transit operators in the United States were randomly screening passengers or baggage every day. However, during the Democratic National Convention in 2004, MBTA began randomly screening every 11th passenger at certain stations and times of the day, asking the passenger to provide his or her bags to be screened. Those who refused were not allowed to ride the system. MBTA officials recognized that it is impossible to implement such a system comprehensively throughout the rail network without major staffing increases, and that even doing random screening regularly would be a drain on resources. However, officials stated that such a system is workable during special events and times of heightened security but would have to be designed very carefully to ensure that passengers' civil liberties were not violated. After the July 2005 London bombings, four rail transit operators—PATH,

New York Metropolitan Transportation Authority, New Jersey Transit, and Utah Transit Authority in Salt Lake City—implemented limited forms of random baggage screening in their system.

National government maintains clearinghouse on technologies and best practices: According to passenger rail operators in five countries we visited, their national governments have centralized the process for performing research and developing passenger rail security technologies and maintaining a clearinghouse on these technologies and security best practices. According to these officials, this practice allows rail operators to have one central source for information on the merits of a particular passenger rail security technology, such as chemical sensors, CCTVs, and intrusion detection devices. No federal agency has compiled or disseminated best practices to rail operators to aid in this process. Some U.S. rail operators we interviewed expressed interest in there being a more active centralized federal research and development authority in the United States to evaluate and certify passenger rail security technologies and make that information available to rail operators. We have also previously reported that stakeholders have stated that the federal government should play a greater role in testing transportation security technology and making this information available to industry stakeholders.[9] Currently, many operators said they informally ask other rail operators about their experiences with a certain technology, perform their own research via the Internet or trade publications, or perform their own testing. TSA and DOT agree that making the results of research testing available to industry stakeholders could be a valuable use of federal resources because it would reduce the need for multiple rail operators to perform the same research and development efforts, but they have not taken steps to implement this practice.[10]

Implementing these three practices—covert testing, random screening, and a government-sponsored clearinghouse for technologies and best practices—in the United States could pose political, legal, fiscal, and cultural challenges because of the differences between the United States and these foreign nations. For instance, many foreign nations have dealt with terrorist attacks on their public transportation systems for decades, compared with the United States, where rail transportation has not been

[9]GAO-03-843.

[10]GAO-03-843.

specifically targeted during terrorist attacks. According to foreign rail operators, these experiences have resulted in greater acceptance of certain security practices, such as random searches, which the U.S. public may view as a violation of their civil liberties or which may discourage the use of public transportation. The impact of security measures on passengers is an important consideration for domestic rail transit operators, since most passengers could choose another means of transportation, such as a personal automobile. As such, security measures that limit accessibility, cause delays, increase fares, or otherwise cause inconvenience could push people away from transit and into their cars. In contrast, the citizens of the European and Asian countries we visited are more dependent on public transportation than most U.S. residents and therefore, according to the rail operators we spoke with, may be more willing to accept more intrusive security measures, simply because they have no other choice for getting from place to place. Nevertheless, in order to identify innovative security measures that could help further mitigate terrorism-related risk to rail assets it is important to at least consider assessing the feasibility and costs and benefits of implementing in the United States 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. Furthermore, the passenger rail association officials told us that such an evaluation should include practices used by foreign rail operators that integrate security into infrastructure design.

Differences in the business models and financial status of some foreign rail operators could also affect the feasibility of adopting certain security practices in the United States. Several foreign countries we visited have privatized their passenger rail operations. Although most of the foreign rail operators we visited—even the privatized systems—rely on their governments for some type of financial assistance, two foreign rail operators generated significant revenue and profits in other business endeavors, which they said allowed them to invest heavily in security measures for their rail systems.

Another important difference between domestic and foreign rail operators is the structure of their police forces. In particular, England, France, Belgium, and Spain all have national police forces patrolling rail systems in these countries. The use of a national police force is a reflection that these foreign countries often have one nationalized rail system, rather than over 30 rail transit systems owned and operated by numerous state and local governments, as is the case in the United States. For example, in

France, the French National Railway operates all intercity passenger rail services in the country, and the French Railway police provide security. According to foreign rail operators, the use of one national rail police force allows for consistent policing and security measures throughout the country. In the United States, by contrast, some transit agencies maintain individual polices forces, while others rely on their city or county police forces for security.

DHS and DOT Help Fund Security Efforts, and Some Funding Decisions Are Risk-Based

Both DHS and DOT help fund rail transit security investments, and DHS has promoted risk-based funding decisions in the allocation of transit security grants. DHS's Office of Grants and Training administers the UASI and Transit Security grant programs. These programs have provided over $320 million in grants to rail transit agencies for certain security activities since fiscal year 2003. The Office of Grants and Training has leveraged its grant-making authority to promote risk-based funding decisions for passenger rail by requiring, for example, that operators complete a risk assessment to be eligible for a transit security grant. FTA also helps fund rail transit security efforts through the financial assistance it provides to transit agencies, with the stipulation that a certain percentage of federal funds be used for security activities.

DHS and DOT Help Fund Rail Transit Security Efforts

With the creation of DHS in 2002, one of its components, the Office of Grants and Training, became the primary federal source for security funding for passenger rail systems. The Office of Grants and Training is the principal component of DHS responsible for preparing the United States for acts of terrorism and has primary responsibility within the executive branch for assisting and supporting DHS, in coordination with other directorates and entities outside the department, in conducting risk analysis and risk management activities for state and local governments. In carrying out its mission, the Office of Grants and Training provides training, funds for the purchase of equipment, support for the planning and execution of exercises, technical assistance, and other support to assist states, local jurisdictions, and the private sector to prevent, prepare for, and respond to acts of terrorism. Through the UASI grant program, the Office of Grants and Training has provided grants to urban areas to help enhance their overall security and preparedness level to prevent, respond to, and recover from acts of terrorism. In 2003 and 2004, $65 million and $50 million, respectively, were allocated to rail transit agencies through

the UASI program. In addition, the DHS Appropriations Act of 2005 appropriated $150 million for rail transit, intercity passenger rail, freight rail, and transit agency security grants.[11] This funding has allowed the Office of Grants and Training to build upon 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. This program provides financial assistance to address security preparedness and enhancements for transit (to include commuter, heavy, and light rail systems; intracity buses, and ferries). Table 1 summarizes the funding provided to rail transit providers through the UASI and Transit Security Grant Program from 2003 through 2006.

Table 1: Security Grants Provided by the Office of Grants and Training to Rail Transit Providers, 2003 through 2006

Fiscal year	Funding levels
2003	$65,000,000
2004	$50,000,000
2005	$108,000,000
2006	$110,000,000
Total	**$323,000,000**

Source: DHS Office of Grants and Training.

Although FTA now plays a supporting role in rail transit security matters since the creation of TSA, it remains an important partner in funding security efforts. FTA provides financial assistance to rail transit agencies to plan and develop new systems and operate, maintain, and improve existing systems. Rail transit agencies can use some of this funding for security activities, although the agencies have to balance investments in security against other competing priorities. In addition, FTA promotes safety and security through its grant-making authority. FTA stipulates conditions of grants, such as certain safety and security statutory and regulatory requirements, and FTA may withhold funds for noncompliance with the conditions of a grant. For example, transit agencies must spend 1

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

percent of their urbanized area formula funds—which is FTA's largest grant program—on security improvements.[12]

Using Risk Management Approach Can Help Direct Federal Funds to Highest Rail Transit Security Priorities

In recent years, we, along with Congress, the executive branch, and the 9/11 Commission have required or advocated that federal agencies with homeland security responsibilities use a risk management approach to help ensure that finite national resources are dedicated to assets or activities considered to have the highest security priority. A risk management approach entails a continuous process of managing risk through a series of actions, including setting strategic goals and objectives, performing risk assessments, evaluating alternative actions to reduce identified risks by preventing or mitigating their impact, selecting actions to undertake by management, and implementing and monitoring those actions. We have concluded that without a risk management approach, there is limited assurance that programs designed to combat terrorism are properly prioritized and focused. Targeting resources to the highest priority is especially critical given the competition for resources within the rail transit sector, and between the rail transit sector and the other modes of transportation. Moreover, as the 2005 London rail bombings dramatically illustrated, even when a variety of security precautions are put in place, passenger rail systems remain vulnerable and attractive targets given their open designs and the high volumes of passengers they transport each day. Thus, it is important that limited resources are targeted to security activities that have the greatest impact on reducing overall risk.

DHS' Office of Grants and Training has leveraged its grant-making authority to promote risk-based funding decisions for passenger rail. For example, passenger rail operators must have completed a risk assessment to be eligible for financial assistance through the fiscal year 2005 Transit Security Grant program administered by the Office of Grants and Training. To receive these funds, rail transit 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

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

assessments. This plan, along with a regional transit security strategy prepared by regional transit stakeholders, will serve as the basis for determining how the grant funds are to be allocated.

Coordination between Federal Agencies Has Faced Challenges and Will Continue to Be Important

Prior to the creation of DHS, DOT modal agencies, such as FTA and FRA, were the primary federal agencies involved in rail transit security matters. Since Congress passed ATSA in 2001, creating TSA and giving it regulatory authority over the security of all modes of transportation, federal agencies have had some difficulty coordinating their activities and communicating to industry stakeholders about their role and responsibilities. In response to a GAO recommendation, DOT and DHS entered into an MOU to better coordinate their activities and have embarked on a number of initiatives to improve their coordination with each other and with industry stakeholders. Coordination between DHS and DOT will continue to be important as both departments move forward with existing programs and new security initiatives, such as TSA's deployment of its rail inspectors.

DHS and DOT Have Worked to Improve Coordination on Transit Security Matters

Although DOT modal administrations have played supporting roles in transportation security matters since the creation of TSA, they remain important partners in the federal government's efforts to improve rail security, given DOT's role in funding and overseeing the safety of rail transit systems. For example, as previously mentioned, FTA provides financial assistance to rail transit agencies, and some of this funding can, and in some cases must, be used for security activities. In addition, FTA has regulatory authority for state safety oversight of rail fixed-guideway systems and for a drug and alcohol program, and FRA has regulatory authority for rail safety over commuter rail operators. As we have previously reported, it could be difficult to distinguish DOT's role in maintaining and improving transportation safety from DHS's role in securing the transportation system because security is often intertwined with safety.[13] Moreover, FTA and FRA are continuing their rail transit security efforts as TSA moves ahead with its rail transit security initiatives.[14]

[13]GAO-03-843.

[14]For information about TSA's, FTA's, and FRA's rail transit security initiatives, see GAO-05-851.

We have previously reported that coordination between DHS and DOT, as well as between DHS and rail transit stakeholders, could be improved. For example, in our September 2005 report on rail security, we noted that TSA provided limited opportunities for other federal agencies and the rail industry to collaborate in the development of its passenger rail security directives, which were issued in May 2004 to provide a consistent baseline standard of protective measures for all passenger rail operators.[15] Federal and rail industry officials have raised questions about the feasibility of implementing and complying with the directives, noting, among other things, that the directives do not reflect a complete understanding of the rail transit environment or necessarily incorporate industry best practices. In addition, in 2003, we noted that representatives from several associations told us that they have received conflicting messages from the federal agencies involved in transportation security, including rail transit.[16] We further noted that representatives from several associations also stated that their members were unclear about which agency to contact for their various security concerns and which agency has oversight for certain issues. We concluded that a lack of clearly defined roles and responsibilities can lead to problems such as duplication and conflicting efforts, gaps in preparedness, and confusion. Moreover, a lack of coordination can strain intergovernmental relationships, drain resources, and raise the potential for problems in responding to terrorism. Therefore, we recommended that DHS and DOT use a mechanism, such as a memorandum of agreement, to clearly delineate their roles and responsibilities. At a minimum, we recommended that this mechanism establish the responsibilities of each entity in setting, administering, and implementing security standards and regulations; determining funding priorities; and interfacing with the transportation industry, as well as define each entity's role in the inevitable overlap of some safety and security activities.

In response to our 2003 recommendation, DHS and DOT signed a memorandum of understanding (MOU) in September 2004 to develop procedures through which the two departments could improve their cooperation and coordination in 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

[15]GAO-05-851.

[16]GAO-03-843.

stakeholders, will identify, prioritize, and coordinate the protection of critical infrastructure. The MOU between DHS and DOT represents an overall framework for cooperation that is to be supplemented by additional signed agreements, or annexes, between the departments. These annexes are to delineate the specific security-related roles, responsibilities, resources, and commitments for mass transit, rail, research and development, and other matters. The annex for mass transit security was signed in September 2005.[17] According to DHS and DOT officials, this annex is intended to ensure that the programs and protocols for incorporating stakeholder feedback and making enhancements to security measures are coordinated. For example, the annex requires that DHS and DOT consult on such matters as regulations and directives that affect security. The annex also identifies points of contact for coordinating this consultation.

In addition to their work on the MOU and related annexes, DHS and TSA have taken other steps to improve collaboration with DOT and industry stakeholders. In April 2005, DHS officials stated that better collaboration with DOT and industry stakeholders was needed to develop strategic security plans associated with various homeland security presidential directives and statutory mandates, such as the Intelligence Reform and Terrorism Prevention Act of 2004, which required DHS to develop a national strategy for transportation security in conjunction with DOT. Responding to the need for better collaboration, DHS established a senior-level steering committee in conjunction with DOT to coordinate the development of this national strategy. In addition, senior DHS and TSA officials stated that industry groups would also be involved in developing the national strategy for transportation security and other strategic plans. Moreover, according to TSA's assistant administrator for intermodal programs, TSA intends to work with APTA and other industry stakeholders in developing security standards for the rail transit industry.[18]

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

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

Coordination between Federal Agencies Will Continue to Be Important

DOT's and DHS's efforts to enhance coordination between their agencies and with industry stakeholders on security matters are welcome. Effective coordination between the two departments will continue to be important as both move forward in implementing existing programs as well as new security initiatives. For example, FTA administers the State Safety Oversight program, which mandates that state-designated agencies oversee the safety of rail transit agencies. Although ATSA gave TSA final regulatory authority over all modes of transportation, including rail transit, in the program, FTA sets out minimum requirements the state oversight agencies must ensure that transit agencies meet. FTA's mandated minimum requirements include security components, one of which directs rail transit agencies to maintain a system security plan that includes controls to address employee and passenger security and a process for conducting internal security reviews. Several rail transit operators told us that they were confused by having to answer to both FTA and TSA for transportation security matters. We have ongoing work for the full Committee examining the State Safety Oversight program—and, as part of this review, we will be exploring the extent to which FTA and TSA work together in implementing this program. We expect to issue our report later this summer.

Another area that will require continued coordination is DHS's and DOT's security and safety oversight efforts. TSA has hired rail inspectors to, among other things, monitor and enforce compliance with its May 2004 passenger rail security directives. As of March 2006, TSA had filled 99 of up to 100 inspector positions authorized by Congress.[19] However, TSA has not yet established processes or criteria for determining and enforcing compliance. TSA has also not determined how its rail inspectors will be used to enforce the directives or how they will coordinate with existing FRA safety inspectors or state oversight auditors involved in the State Safety Oversight Program. The Director of TSA's Surface Transportation Inspection Program, which oversees the rail inspectors, and a local rail inspector program supervisor told us that they looked forward to coordinating with FTA on the State Safety Oversight program and would be open to a formalized role in the program, but had not held any discussions with FTA about what that role would be. In fact, both the Director and the local supervisor admitted that they were not familiar with the program's requirements. In addition, the transit security annex to the

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

MOU between DHS and DOT does not explicitly mention the State Safety Oversight program as a program for which the two agencies will collaborate, and officials from several state oversight agencies said they were unsure what their role would be in overseeing security once the TSA rail inspectors began their duties. Also, FRA and TSA officials told us that the details of how TSA rail inspectors will coordinate with the approximately 400 existing FRA safety inspectors and 160 state employees enforcing FRA passenger rail rules and regulations remain to be determined. Both FRA and TSA stated that they were committed to avoiding duplication of effort and would work to communicate their respective roles and responsibilities to transit agency officials.

Another area requiring continued coordination is the funding of rail transit security activities. Specifically, the Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users (SAFETEA-LU)[20] included a provision mandating that DOT and DHS collaborate on a joint rulemaking for the Transit Security Grant Program. The joint rulemaking is to establish the characteristics of and requirements for transit security grants, including funding priorities, eligible activities, methods for awarding grants, and limitations on administrative expenses. The rule is currently being drafted, and officials from DHS' Office of Grants and Training told us they expected it to be finalized in summer 2006.

Concluding Observations

In conclusion, Mr. Chairman, the 2005 London rail bombings made clear that even when a variety of security precautions are put in place, rail transit systems that move high volumes of passengers daily remain vulnerable to attack. Security cannot be guaranteed. Nevertheless, it is important that we take steps to identify and mitigate risks to passenger rail systems. While domestic rail agencies have implemented a number of security practices that are generally consistent with those of foreign rail operators, they have not adopted some practices used in other countries, including covert testing, random screening, and information clearinghouses for new security technologies and best practices. Despite the potential political, legal, fiscal, and cultural challenges that implementing these additional practices in the United States could pose, we continue to believe that the practices may warrant further examination, and we stand by our September 2005 recommendations that DHS, in collaboration with DOT and the passenger rail industry, evaluate the feasibility of implementing them.

[20]P.L. 109-59.

As we move forward with efforts to enhance rail transit security, it is important that we do not examine rail transit security actions and funding in isolation. Rail transit systems represent one of many modes of transportation competing for limited federal security resources. Given competing priorities and finite resources, difficult policy decisions will have to be made by Congress and the executive branch to prioritize security efforts and direct resources to the areas of greatest risk within the passenger rail system, across all transportation modes, and across other sectors of the economy. As we have previously noted in past reports, adopting a risk management approach can help guide and inform these difficult decisions—and help ensure that finite national resources are dedicated to assets or activities considered to have the highest security priority. DHS has taken steps to adopt a risk management approach.

Finally, the sheer number of stakeholders involved in securing rail transit systems can lead to communication challenges, duplication of effort, and confusion about roles and responsibilities. With the execution of the MOU and transit security annex, DHS and DOT have taken important steps forward in improving coordination among the federal entities involved in rail transit security matters. These new agreements will be tested as both departments proceed with new security initiatives and existing programs, such as FTA's State Safety Oversight program. We stand ready to assist the Committee and Subcommittee in monitoring these developments.

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

Contact Information

For further information on this testimony, please contact JayEtta Z. Hecker at (202) 512-2834 or Cathleen A. Berrick at (202) 512- 3404. Individuals making key contributions to this testimony include Nikki Clowers, Colin Fallon, Kirk Kiester, and Ray Sendejas.

Appendix I—Domestic and Foreign Rail Agencies GAO Contacted for GAO-05-851

Table 1: Domestic Passenger Rail Agencies We Visited or Interviewed

Passenger rail agency	Urban area served
Altamont Commuter Express (ACE)	Stockton and San Jose, California
Alaska Railroad Corporation	Anchorage and Fairbanks, Alaska
Bay Area Rapid Transit (BART)	San Francisco – Oakland, California
CALTRAIN	San Francisco and San Jose, California
San Diego Transit Corp. (Coaster)	San Diego, California
Dallas Area Rapid Transit / Trinity Railway Express (DART)	Dallas, Texas
Greater Cleveland Regional Transportation Authority (GCRTA)	Cleveland, Ohio
Los Angeles County Metropolitan Transportation Authority (LACMTA)	Los Angeles, California
Metropolitan Atlanta Rapid Transit Authority (MARTA)	Atlanta, Georgia
Maryland Transit Administration (MTA)	Greater Washington, DC, and Maryland
Massachusetts Bay Transportation Authority (MBTA)	Boston, Massachusetts
METRA Commuter Rail	Chicago, Illinois
Southern California Regional Rail Authority (Metrolink)	Greater Los Angeles, California
Long Island Railroad (LIRR)	New York, New York
Metro North Railroad (MNR)	New York, New York
New York City Transit (NYCT)	New York, New York
Staten Island Railway (SIR)	New York, New York
San Francisco Municipal Railway (MUNI)	San Francisco, California
Northern Indiana Commuter District	Chicago, Illinois –- Northern Indiana
Delaware River Port Authority (PATCO)	New Jersey and Philadelphia, Pennsylvania
Port Authority Trans Hudson (PATH)	New York, New York –- New Jersey
San Diego Trolley	San Diego, California
Southeastern Pennsylvania Transportation Authority (SEPTA)	Philadelphia, Pennsylvania

Passenger rail agency	Urban area served
South Florida Regional Transportation Authority (SFRTA)	Miami, Florida
Connecticut Department of Transportation (Shore Line East)	New Haven, Connecticut
Sound Transit (Sounder)	Seattle, Washington
TRIMET	Portland, Oregon
Virginia Railway Express (VRE)	Northern Virginia, Greater Washington, D.C.
Washington Metropolitan Area Transit Authority (WMATA)	Washington, D.C.
New Jersey Transit (NJT)	Newark, New Jersey –- New York, New York
Miami Dade Transit	Miami, Florida
Chicago Transit Authority (CTA)	Chicago, Illinois

Source: National Transit Database

Table 2: Foreign Passenger Agencies We Contacted

Passenger rail agency	Area served
Paris Metro	Paris, France
French National Railway	France
London Underground	London, United Kingdom
Network Rail	United Kingdom
Channel Tunnel Rail Link	United Kingdom/France
Belgian National Railway	Belgium
Madrid Metro	Madrid, Spain
RENFE (Spanish National Railway)	Spain
JR Central	Japan
Tokyo Metro	Tokyo, Japan
SBS Transit Corporation	Singapore
Singapore Mass Rapid Transit	Singapore
Hong Kong Mass Transit Railway	Hong Kong

Source: GAO

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