United States Government Accountability Office

GAO

Testimony

Before the Committee on Commerce, Science, and Transportation, U.S. Senate

For Release on Delivery
Expected at 2:30 p.m. EDT
Tuesday, June 14, 2011

RAIL SECURITY

TSA Improved Risk Assessment but Could Further Improve Training and Information Sharing

Statement of Steve Lord, Director
Homeland Security and Justice Issues

GAO-11-688T

June 14, 2011

RAIL SECURITY

TSA Improved Risk Assessment but Could Further Improve Training and Information Sharing

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-11-688T, a testimony before the Committee on Commerce, Science, and Transportation, U.S. Senate

Why GAO Did This Study

Alleged terrorist plots against rail systems in major U.S. cities have increased focus on these systems. The Transportation Security Administration (TSA), within the Department of Homeland Security (DHS), is the primary federal agency responsible for rail security. This testimony addresses the following: (1) the extent that DHS has conducted comprehensive risk assessments for the transportation sector, including for rail, (2) technologies available to enhance rail security, (3) TSA's efforts regarding rail security training, and (4) rail stakeholders' satisfaction with security-related information TSA is providing. GAO's testimony is based on GAO reports issued from March 2009 through September 2010, selected updates conducted in May through June 2011, and preliminary results from ongoing work on information sharing. As part of the ongoing work, GAO surveyed the seven largest freight rail carriers (based on revenue) and interviewed security officials from three of these rail carriers selected for location, as well as TSA officials.

What GAO Recommends

GAO has made recommendations in prior work to enhance DHS's and TSA's rail security efforts. DHS generally concurred with the recommendations and has actions under way to address them. DHS generally agreed with the preliminary observations in this statement, and provided technical comments, which were incorporated as appropriate.

View GAO-11-688T or key components. For more information, contact Steve Lord at (202) 512-8777 or lords@gao.gov.

What GAO Found

TSA has taken steps to conduct comprehensive risk assessments across the transportation sector and within passenger and freight rail modes that combine the three elements of risk—threat, vulnerability, and consequence. For example, in March 2009, GAO reported that TSA had taken actions to implement a risk management approach but had not conducted comprehensive risk assessments for the transportation sector as a whole, and recommended that TSA do so to help ensure that resources are allocated to the highest-priority risks. DHS concurred and in June 2010 produced the Transportation Sector Security Risk Assessment, which assessed risk as a factor of all three risk elements within and across the transportation sector, including rail. GAO has also made recommendations to strengthen risk assessments within individual modes, such as expanding TSA's efforts to include all security threats in its freight rail assessments, including potential sabotage to bridges, tunnels, and other critical infrastructure. DHS concurred and is addressing the recommendations.

Several technologies are available to address rail security, such as security cameras, handheld explosive trace detection systems, x-raying imaging systems, and canines. However, technologies are at varying levels of maturity and involve trade-offs in mobility, cost, and privacy. In July 2010, for example, we reported that the ability of explosives detection technologies to help protect the passenger rail environment depends on detection performance and how effectively they can be deployed.

TSA has not issued regulations for public transportation and railroad security training programs, as required by the Implementing Recommendations of the 9/11 Commission Act of 2007. In June 2009, GAO reported that TSA had not implemented the training requirement and recommended that DHS develop a plan with milestones for doing so, as called for by project management best practices. DHS concurred, and in June 2011 TSA stated that it had developed a timeline for uncompleted 9/11 Commission Act requirements. TSA also stated that it is finalizing the security training program regulations and expects to issue a Notice of Proposed Rulemaking for public comment by November 2011.

Opportunities exist to streamline security information for transit agencies, and preliminary results of ongoing work indicate that some freight rail agencies do not receive actionable information from TSA. In September 2010, GAO recommended that DHS assess opportunities to streamline information-sharing mechanisms to reduce overlap. DHS concurred, and in response it and the rail industry have developed a streamlined product. However, preliminary observations from GAO's ongoing work indicate that some rail stakeholders would prefer to receive actionable security information and analysis from TSA that could allow them to adjust to potential terrorist threats. TSA officials agreed that improvements are needed in the products and mechanisms by which they alert rail agencies of security-related information. GAO will continue to monitor this issue and expects to issue a report by the end of 2011.

Chairman Rockefeller, Ranking Member Hutchison, and Members of the Committee:

I appreciate the opportunity to participate in today's hearing to discuss security issues related to the U.S. rail system, including mass transit, intercity passenger rail (Amtrak), and freight rail. Rail systems in the United States have received heightened attention as several alleged terrorists' plots have been uncovered, including plots against transit systems in the New York City and Washington, D.C., areas. Intelligence recovered from Osama bin Laden's compound indicates that U.S. rail systems were a suggested target as recently as February 2010, although there has been no indication of a specific or imminent threat to carry out such an attack. Terrorist attacks on rail systems around the world—such as the March 2010 Moscow, Russia, subway bombings, and the May 2010 passenger train derailment near Mumbai, India, that resulted in approximately 150 fatalities—highlight the vulnerability of these systems to terrorist attacks. Further, the Mineta Transportation Institute has reported that terrorists attempted to derail trains on at least 144 occasions between 1995 and 2010, many of which were in South Asia and mostly through the use of track bombs.[1]

One of the critical challenges facing rail system operators—and the federal agencies that regulate and oversee them—is finding ways to protect rail systems from potential terrorist attacks without compromising the accessibility and efficiency of rail travel. The systems are vulnerable to attack in part because they rely on an open architecture that is difficult to monitor and secure due to its multiple access points, hubs serving multiple carriers, and, in some cases, no barriers to access. Further, rail systems' high ridership, expensive infrastructure, economic importance, and location in large metropolitan areas or tourist destinations make them attractive targets for terrorists. In addition, the multiple access points along extended routes make the costs of securing each location potentially prohibitive.

My testimony today focuses on the following issues: (1) To what extent has the Department of Homeland Security (DHS) conducted

[1]The Norman Y. Mineta International Institute for Surface Transportation Policy Studies was established by the Intermodal Surface Transportation Efficiency Act of 1991. Pub. L. No. 102-240, § 6024, 105 Stat. 1914 (1991). The institute's transportation policy work is centered on, among other things, research into transportation security, planning, and policy development.

comprehensive risk assessments to inform its security efforts across all modes of transportation, including rail? (2) What technologies are available to assist rail operators in securing their systems? (3) What is the status of Transportation Security Administration's (TSA) efforts regarding security training for frontline rail employees? (4) How satisfied are rail stakeholders with the quality of security-related information TSA is providing?

This statement is based on related GAO reports issued from March 2009 through September 2010, including selected updates conducted from May 2011 through June 2011 on TSA's efforts to implement our prior recommendations regarding surface transportation security.[2] In conducting these updates, we obtained information from TSA regarding the agency's efforts to develop regulations for security training programs for rail employees and to enhance its overall risk management approach to rail security, among other things. Our previous reports incorporated information we obtained and analyzed from officials from various components of DHS, the Department of Transportation (DOT), state and local transportation and law enforcement agencies, and industry associations, as well as a survey of 96 U.S. public transit agencies (that represented about 91 percent of total 2008 ridership). Our previously published products contain additional details on the scope and methodology, including data reliability, for those reviews. In addition, this statement includes preliminary observations based on ongoing work, the results of which will be issued in a report later this year, assessing the extent to which freight rail carriers that receive security-related information are satisfied with the products and mechanisms that TSA uses to disseminate this information, among other things.[3] As part of this ongoing work, we surveyed all seven Class I freight rail carriers.[4] We also interviewed security officials from three Class I freight rail carriers

[2]Surface transportation security includes the mass transit and passenger rail, freight rail, highway and commercial vehicle, and pipeline modes. Please see the list of related products at the end of this testimony statement.

[3]This work is being conducted in response to a mandate in the Implementing Recommendations of the 9/11 Commission Act (9/11 Commission Act). Pub. L. No. 110-53, § 1203(a), 121 Stat. 266, 383 (2007).

[4]As defined by revenue, for 2009, Class I railroads are freight rail carriers having annual operating revenues of $379 million or more. See 49 C.F.R. pt. 1201, General Instructions 1-1. The railroads include CSX Transportation (CSX), BNSF Railway Company (BNSF), Union Pacific Railroad Company (Union Pacific), Norfolk Southern, Kansas City Southern Railway Company, Canadian National Railway, and Canadian Pacific Railway.

selected on the basis of their location. While the results of our interviews are not generalizable to all Class I rail carriers, the responses provide perspectives and examples to expand on survey findings. All of our work was conducted in accordance with generally accepted government auditing standards. These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings based on our audit objectives. For new information that was based on work not previously reported, we obtained TSA views on our findings and incorporated technical comments where appropriate.

Background

TSA is the primary federal agency responsible for overseeing the security of the mass transit, passenger rail, and freight rail systems. However, several other agencies, including DOT's Federal Transit Administration (FTA) and Federal Railroad Administration (FRA), also play a role in helping to oversee these systems. Since it is not practical or feasible to protect all assets and systems against every possible terrorist threat, DHS has called for using risk-informed approaches to prioritize its security-related investments and for developing plans and allocating resources in a way that balances security and commerce.[5]

In June 2006, DHS issued the National Infrastructure Protection Plan (NIPP), which established a six-step risk management framework to establish national priorities, goals, and requirements for Critical Infrastructure and Key Resources protection so that federal funding and resources are applied in the most cost-effective manner to deter threats, reduce vulnerabilities, and minimize the consequences of attacks and other incidents. The NIPP, updated in 2009, defines risk as a function of three elements:

- threat—an indication of the likelihood that a specific type of attack will be initiated against a specific target or class of targets;
- vulnerability—the probability that a particular attempted attack will succeed against a particular target or class of targets; and
- consequence—the effect of a successful attack.

[5]A risk management approach 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.

In August 2007, the Implementing Recommendations of the 9/11 Commission Act (9/11 Commission Act) was signed into law, which included provisions that task DHS with actions related to surface transportation security.[6] Among other things, these provisions include mandates for developing and issuing regulations for transportation security training programs and ensuring that transportation modal security plans include threats, vulnerabilities, and consequences for transportation infrastructure assets including rail.

TSA Has Made Progress in Conducting Comprehensive Risk Assessments across All Modes of Transportation, Including Rail

In response to our previous recommendations, TSA has taken steps to conduct comprehensive risk assessments across the transportation sector and within the passenger and freight rail modes that are based on assessments of threat, vulnerability, and consequence. In March 2009, we reported that TSA had taken some actions to implement a risk management approach but had not conducted comprehensive risk assessments that integrate threat, vulnerability, and consequence for each mode or the transportation sector as a whole, as called for by the NIPP.[7] We recommended that TSA conduct risk assessments that combine these three elements to help the agency produce a comparative analysis of risk across the entire transportation sector, which the agency could use to inform current and future investment decisions.

DHS concurred with this recommendation, and in June 2010 TSA produced the Transportation Sector Security Risk Assessment (TSSRA), which assessed risk within and across the various aviation and surface transportation modes, including rail, and incorporated threat, vulnerability, and consequence.[8] A September 2009 letter from the Director of DHS's Office of Risk Management and Analysis noted that in developing the TSSRA, TSA was making progress toward developing a strategic and comprehensive risk management approach that would better align with DHS's risk management framework and address our

[6]Pub. L. No. 110-53, 121 Stat. 266 (2007).

[7]GAO, *Transportation Security: Comprehensive Risk Assessments and Stronger Internal Controls Needed to Help Inform TSA Resource Allocation*, GAO-09-492 (Washington, D.C.: Mar. 27, 2009).

[8]According to TSA officials, passenger rail is included with mass transit in the TSSRA, although Amtrak is not listed in the TSSRA report as a participant. In June 2011, TSA officials stated that passenger rail would be more clearly broken out in the next version of TSSRA.

recommendations. However, TSA noted limitations in the June 2010 TSSRA report that could limit its usefulness in guiding investment decisions across the transportation sector as a whole. For example, the TSSRA excluded the maritime sector and certain types of threats, such as from "lone wolf" operators. In June 2011, agency officials stated that TSA is working to address these limitations in the next version, which is scheduled for completion by the end of calendar year 2011. TSA also said that it is strengthening and enhancing the TSSRA methodology based on an ongoing independent verification and validation that is scheduled for completion later this year. In addition, TSA officials noted that other DHS components, such as the U.S. Coast Guard, conduct risk assessments of the maritime sector that complement the TSSRA.[9]

With regard to assessments of mass transit and passenger rail transportation, we reported in June 2009 that although TSA had contributed to DHS's risk assessment effort, it had not conducted its own risk assessment of mass transit and passenger rail systems.[10] We recommended that TSA conduct a risk assessment that integrates all three elements of risk. DHS officials concurred with the recommendation, and in March 2010 said that they had developed a mass transit risk assessment tool to assess risk to mass transit and passenger rail systems using threat, vulnerability, and consequence, in addition to the TSSRA. According to TSA, they have completed pilot tests of this tool on three transit systems as of June 2011 and anticipate assessing six additional transit systems by the end of the calendar year.

Similarly, in April 2009, we reported that TSA's efforts to address freight rail security were limited and did not focus on a range of threats identified by federal and industry assessments.[11] TSA's security efforts focused almost entirely on transportation of Toxic Inhalation Hazards (TIH);

[9]We have reviewed the U.S. Coast Guard's risk assessment model as part of previous work. For example, see GAO, *Maritime Security: DHS Progress and Challenges in Key Areas of Port Security*, GAO-10-940T (Washington, D.C.: July 21, 2010). We are also reviewing it as part of our current review of integrated port security being conducted for your committee and expect to issue a report on the results of this effort later this year.

[10]GAO, *Transportation Security: Key Actions Have Been Taken to Enhance Mass Transit and Passenger Rail Security, but Opportunities Exist to Strengthen Federal Strategy and Programs*, GAO-09-678 (Washington, D.C.: June 24, 2009).

[11]GAO, *Freight Rail Security: Actions Have Been Taken to Enhance Security, but the Federal Strategy Can Be Strengthened and Security Efforts Better Monitored*, GAO-09-243 (Washington, D.C.: April 21, 2009).

however, other federal and industry assessments had identified additional potential security threats, such as risks to bridges and tunnels.[12] We reported that although TSA's focus on TIH had been a reasonable initial approach, there are other security threats for TSA to consider and evaluate, including potential sabotage to critical infrastructure. We recommended that TSA expand its efforts to include all security threats in its freight rail security strategy. TSA concurred and reported that it had developed a Critical Infrastructure Risk Tool to measure the criticality and vulnerability of freight railroad bridges. As of June 2011, the agency has used this tool to assess 77 bridges, some of which transverse either the Mississippi or Missouri Rivers, and 26 freight rail tunnels.

Our prior work has also assessed TSA's efforts to incorporate risk management principles into the grant allocation process, and we reported that transit grant funding decisions could be improved with better assessments of vulnerability. For example, we reported in June 2009 that the Transit Security Grant Program (TSGP) risk model included all three elements of risk, but could be strengthened by measuring variations in vulnerability.[13] DHS held vulnerability constant in its assessments, which limits the model's overall ability to assess risk. We recommended that DHS strengthen its methodology for determining risk by developing a cost-effective method for incorporating vulnerability information in its TSGP risk model. DHS concurred with the recommendation, and in April 2010 TSA stated that it is reevaluating the risk model for the fiscal year 2011 grant cycle. In June 2011, TSA stated that it is considering asset-specific vulnerability when looking at risk, although TSA noted that the Federal Emergency Management Agency (FEMA) has ownership of the TSGP risk model. TSA provides input into the model, however. We are currently assessing DHS and FEMA efforts to improve the TSGP grant-allocation process as part of our current review of DHS grant programs being

[12]TIH include chlorine and anhydrous ammonia, which can be fatal if inhaled. Shipments of TIH, especially chlorine, frequently move through densely populated areas to reach, for example, water treatment facilities that use these products. We reported that TSA focused on securing TIH materials for several reasons, including limited resources and a decision in 2004 to prioritize TIH as a key risk requiring federal attention. Other federal and industry freight rail stakeholders agreed that focusing on TIH was a sound initial strategy because it is a key potential rail security threat and an overall transportation safety concern.

[13]GAO, *Transit Security Grant Program: DHS Allocates Grants Based on Risk, but Its Risk Methodology, Management Controls, and Grant Oversight Can Be Strengthened*, GAO-09-491 (Washington, D.C.: June 2009). The TSGP provides grant funding to the nation's key high-threat urban areas to enhance security measures for their critical transit infrastructure, including rail systems.

conducted for your committee and expect to issue a report on the results of this effort later this year.

Technologies Are Available to Strengthen Rail Security, but Challenges in the Rail Environment and Low Maturity of Some Technologies May Limit Implementation

Industry stakeholders have examined and implemented various technologies to enhance the security of the rail system. For example, in April 2009, we reported that several freight rail carriers we met with installed security cameras and monitoring equipment at some of their key facilities to better monitor the activities in and around these areas.[14] We also reported that officials from three railroads and two chemical companies we met with stated that they had taken steps to attempt to better track the movements of their TIH rail shipments by installing Global Positioning System technology on their locomotives and tank cars. Similarly, in June 2009, we reported that many mass transit and passenger rail agencies reported making capital improvements to secure their systems.[15] For example, 19 of the 30 transit agencies we interviewed had embarked on programs since 2004 to upgrade their existing security technology, including upgrading closed circuit television at key station locations with video surveillance systems that alert personnel to suspicious activities and abandoned packages and installing chemical, biological, radiological, nuclear, and explosives detection equipment and laser intrusion detection systems in critical areas.[16]

While industry has taken these steps to implement technology to enhance rail security, the nature of the rail system has presented challenges to further implementation. For example, we reported in July 2010 that in commuter or light rail systems, many stations may be unmanned outdoor platforms without barriers between public areas and trains.[17] Stations may also have few natural locations to place technologies to be able to screen passengers. With limited existing chokepoints, implementation of certain technologies may require station infrastructure modifications to aid in funneling passengers for screening. Similarly, challenges to using

[14]GAO-09-243.

[15]GAO-09-678.

[16]We also reported that TSA collaborates with DHS's Science and Technology Directorate to research, develop, and test various security technologies for applicability in mass transit and passenger rail systems, including explosive trace detection technologies, infrastructure protection measures, and behavior based and advanced imaging technologies.

[17]GAO, *Technology Assessment: Explosives Detection Technologies to Protect Passenger Rail*, GAO-10-898 (Washington, D.C.: July 28, 2010).

technology to secure the freight rail system include the size and open nature of the system, the need for railcars to be able to continuously move, and limited resources.

We have also reported that several technologies are available to help address rail security challenges, but they are at varying levels of maturity and using them involves trade-offs in mobility, cost, and privacy. For example, in July 2010, we reported that the ability of explosives detection technologies to help protect the passenger rail environment depends both upon their detection performance and how effectively the technologies can be deployed in that environment.[18] Detection performance of these technologies varies across the different technologies and additional limitations—such as limited screening throughput, privacy, openness, physical infrastructure, cost, and mobility concerns—have restricted their more widespread or more effective use in passenger rail. More-established explosives detection technologies—such as handheld explosive trace detection systems, x-raying imaging systems, and canines—have demonstrated good performance against many conventional explosives threats but are challenged by threats from certain explosives.[19] Newer technologies—such as Explosive Trace Portals (ETP), standoff detection systems, and Advanced Imaging Technologies (AIT)—while available, are in various stages of maturity and more operational experience would be required to determine whether they can be effectively implemented in a rail environment.[20] For example, AIT technologies have the ability to detect hidden objects; however, they are walk-through devices that would

[18]GAO-10-898.

[19]DHS considers certain details regarding the ability of particular technologies to detect explosives and any limitations in their ability to detect certain types of explosives to be Sensitive Security Information or classified.

[20]ETP are used in screening for access to buildings. The operation of these systems generally involves a screener directing an individual to the ETP and the ETP sensing his presence and, when ready, instructing the individual to enter. The portal then blows short puffs of air onto the individual being screened to help displace particles and attempts to collect these particles with a vacuum system. The particle sample is then preconcentrated and fed into the detector for analysis. Standoff detection systems allow for the screening of rail passengers from a distance. When applied to passenger rail, their distinguishing feature is they attempt to screen passengers with minimal to no effect on normal passenger flow. There is no standard definition of standoff detection and separation distances can be less than a meter to tens of meters and beyond. AIT portals are used for screening people for building access and, to an increasing extent, airport access. The AIT portal then takes images of the individual, which are displayed to another officer who inspects the images. The inspecting officer views the image to determine if there are threats present.

require rail passengers to be funneled through the equipment, limiting passenger throughput with long screening times. Standoff technology can be used to detect hidden objects on an individual from a significant distance and is attractive because it may have less effect on passenger throughput than other new technologies. However, certain types of standoff systems, as well as AIT technologies raise privacy concerns because they create images of individuals underneath their clothing.

In our July 2010 report, we did not make any recommendations regarding the explosives detection technologies available or in development that could help secure passenger rail systems, but we raised various policy considerations. Among other things, we noted that securing passenger rail involves multiple security measures, with explosives detection technologies just one of several components that policymakers can consider as part of the overall security environment. In determining whether and how to implement these technologies, federal agencies and rail operators will likely be confronted with challenges related to the costs versus the benefits of a given technology and the potential privacy and legal implications of using explosives detection technologies.

TSA Has Not Issued Rail Security Training Regulations but Has Provided Funding and Guidance for Training

In 2007 TSA officials identified the need for increased security training at mass transit and passenger rail systems because the extent of training provided varied greatly—with a majority providing an introductory level of safety and security training for new hires, but not refresher training. In addition, TSA identified security awareness training and a lack of a robust, standardized corporate security planning for freight railroads as systematic security gaps. The 9/11 Commission Act mandates TSA to develop and issue regulations for a public transportation security training program and for a railroad security training program.[21] In June 2009, we reported that TSA had not implemented this requirement or several others related to mass transit and passenger rail security, and recommended that DHS develop a plan with milestones for doing so.[22] DHS concurred with this recommendation, and in June 2011, TSA stated that it had developed a plan and milestones for addressing uncompleted 9/11 Commission Act requirements. TSA also stated that it is finalizing the security training program regulations and expects to issue a Notice of Proposed

[21]Pub. L. No. 110-53, §§ 1408, 1517, 121 Stat. 266, 409, 439 (2007).

[22]GAO-09-678.

Rulemaking for public comment by November 2011.[23] A TSA official indicated that the delay was due, in part, to difficulties incurred in trying to address multiple modes of transportation in one regulation.

To address identified training deficiencies, TSA supports security training through its TSGP and voluntary security awareness programs. TSA established a Mass Transit Security Training program in 2007 to provide curriculum guidelines for basic and follow-on security training areas and makes funding available through TSGP.[24] For example, TSA offers mass transit and passenger rail agencies the option of using grant funding to cover costs for training to employees that is supplied by either (1) training providers that are federally funded or sponsored or (2) other training providers.[25] However, in June 2009 we reported that opportunities exist for TSA to strengthen its process for ensuring consistency in the performance of nonfederal training vendors that mass transit and passenger rail agencies use to obtain training through the program.[26] We recommended that to better ensure that DHS consistently funds sound and valid security training delivery programs for mass transit and passenger rail employees, TSA should consider enhancing its criteria for evaluating whether security training vendors meet the performance standards of federally sponsored training providers and whether the nonfederally sponsored providers could be used by transit agencies for training under the transit security grant program. DHS concurred with the recommendation, noting that TSA

[23]Despite the absence of the TSA security training regulations required by the 9/11 Commission Act, railroad organizations are subject to established regulations such as the Pipeline and Hazardous Materials Safety Administration (PHMSA) security training regulations for hazmat (hazardous materials) employees. Among other things, the PHMSA security regulations require that hazmat employee training provide an awareness of security risks associated with hazardous materials transportation and methods designed to enhance transportation security. The training must also include a component covering how to recognize and respond to possible security threats. 49 C.F.R. § 172.704. In addition, FRA regulations require railroads that operate or provide intercity or commuter passenger train service or that host the operation of that service to adopt and comply with a written emergency preparedness plan, which must provide for employee training as well as training of, and coordination with, emergency responders. 49 C.F.R. § 239.101.

[24]DHS also established the Freight Rail Security Grant Program (FRSGP), which provides funds for training programs, among other things.

[25]For 2011, the TSGP prioritizes employee training, drills and exercises, public awareness, and security planning. Among other things, fiscal year 2011 funds may be used for training activities including workshops and conferences and employing contractors to support training related activities.

[26]GAO-09-678.

would work with the FTA through an existing joint working group to develop criteria for reviewing new vendor-provided training courses. In February 2010, TSA stated that it had proposed a joint task group with the FTA to define evaluation criteria for courses submitted by mass transit or passenger rail agencies, academic institutions, or other entities. In June 2011, TSA stated that the joint task group—which is being led by TSA and will include members from the FTA and industry—is in the process of organizing its first meeting. According to TSA, the group will use the criteria it develops to evaluate vendor training courses by the fall of 2011.

DHS, DOT, and others have also taken steps to enhance rail and transit security awareness in partnership with the public and private entities that own and operate the nation's transit and rail systems through voluntary security awareness programs. For example, the Transit Watch Program, co-led by TSA and the FTA, provides a nationwide safety and security awareness program designed to encourage the active participation of transit passengers and employees. By means of this program, the federal government, in collaboration with industry, created templates for transit agencies to develop or enhance their own public awareness programs. In July 2010, DHS launched the "If You See Something, Say Something," campaign as a way to raise public and frontline employee awareness of indicators of terrorism, crime, and other threats and emphasize the importance of reporting suspicious activity to the proper transportation and law enforcement authorities.[27]

[27]The security program was funded, in part, by $13 million from the TSGP and was originally implemented by the New York Metropolitan Transportation Authority.

Opportunities Exist to Streamline Security Information for Transit Agencies, and Preliminary Results Indicate Some Freight Rail Agencies Do Not Receive Actionable Information and Analysis from TSA

While TSA is taking steps to improve information sharing with freight and passenger rail stakeholders, potential overlap could complicate stakeholder efforts to discern relevant information and take appropriate actions to enhance security. In September 2010, we identified the potential for overlap among three federal information-sharing mechanisms: the public transit portal on the Homeland Security Information Network (HSIN-PT), TSA Office of Intelligence's page on HSIN, and the Public Transit Information Sharing and Analysis Center (PT-ISAC).[28] Each of these receives funding from DHS to share security threats and other types of security-related information with public transit agencies. We recommended that DHS establish time frames for a working group of federal and industry officials to assess opportunities to streamline information-sharing mechanisms to reduce any unneeded overlap. DHS concurred with this recommendation.

In response to our recommendation, DHS and the rail industry have taken steps to streamline the information distributed to stakeholders. TSA and key industry groups have developed the Transit and Rail Intelligence Awareness Daily (TRIAD) Report and associated Transportation Information Library. The overall intent of TRIAD is to streamline the analysis, sharing, and exchange of intelligence and security information that had been disseminated by multiple sources. TRIAD includes a daily publication to enhance situational awareness, an alert message to provide immediate awareness of a developing threat or incident, and a catalogue of supporting reports and related documents. According to TSA and its industry partners, HSIN-PT will supplement TRIAD by serving as a reference source to house cross-sector best practices, additional intelligence, and threat information as well as transit security standards and all-hazards information. The TSA Office of Intelligence stated that it will continue to have a portal on HSIN that supplements the information on the PT-ISAC and HSIN-PT. While the TRIAD report may reduce the number of security-related e-mails that transit agencies receive, it does not reduce overlap among the three information-sharing mechanisms. In June 2011, TSA officials stated that they are continuing to coordinate with other members of the working group to identify actions and time frames for addressing our recommendation.

[28]GAO, *Public Transit Security Information Sharing: DHS Could Improve Information Sharing through Streamlining and Increased Outreach*, GAO-10-895 (Washington, D.C.: Sept. 2010).

Our recent work indicates that some rail stakeholders do not receive security information from TSA. In September 2010, we reported that less than half of public transit agencies (34 of 77) responding to our 2010 survey reported that they had log-in access to HSIN, TSA's primary mechanism for sharing open-source security-related information with transportation stakeholders, and had not lost or forgotten their log-in information.[29] Our survey also identified that, of the 19 transit agencies that did not have HSIN access, 12 had never heard of the mechanism, and an additional 11 agencies did not know whether they had access to HSIN. We recommended that TSA establish time frames for the transit-sector public-private working group to conduct targeted outreach efforts to increase awareness of HSIN among agencies that are not currently using or aware of this system. DHS officials concurred with this recommendation and in January 2011 provided an implementation plan with target dates for addressing it. However, the plan was insufficiently detailed for us to determine whether it fully addresses the recommendation. For example, the plan stated that TSA officials created a consolidated "superlist" of current PT-ISAC and HSIN-PT members and transit agencies on a TSA distribution list and intend to encourage all entities on this superlist to join the PT-ISAC and HSIN-PT. However, the plan did not indicate how TSA would target its outreach efforts to those entities not already on one of those lists. In June 2011, a TSA official stated that the public-private working group plans to reach out to other transit entities, such as small agencies, to encourage them to join the PT-ISAC and HSIN-PT. As noted above, TSA officials stated that they are continuing to coordinate with other members of the working group to identify actions and time frames for addressing our recommendation.

Preliminary observations from our ongoing work also indicate that some freight rail stakeholders would prefer to receive more analysis or actionable security information from TSA. The federal government's National Strategy for Information Sharing discusses the need to improve the two-way sharing of terrorism-related information on incidents, threats, consequences, and vulnerabilities, including enhancing the quantity and quality of specific, timely, and actionable information provided by the federal government to critical infrastructure sectors. According to three Class I rail stakeholders that we interviewed, TSA distributes information on rail security that is generally used for situational awareness. However, rail security stakeholders from three of the seven Class I railroads that we

[29] GAO-10-895.

surveyed indicated that TSA's security information products lack analysis, such as trend analysis, that could help predict how certain events may affect freight rail. In follow-up interviews, security officials at three Class I railroads stated that security information provided by TSA does not offer actionable information that could allow them to develop or adjust their current countermeasures against potential terrorist threats. These security officials added that they have often received the same information that TSA provides from the media or other sources before it is distributed from TSA. For example, two of these officials told us that they received little or no security-related information from TSA in the aftermath of Osama bin Laden's death. However, security officials at two of the three rail carriers that we interviewed stated that they felt confident that someone from the federal government would alert them of any direct threat to that carrier. TSA officials agree that improvements are needed in the products and mechanisms by which they alert rail agencies of security-related information and intelligence. For example, a TSA official stated in June 2011 that the agency is in the process of revising its reports on suspicious incidents to regionalize the information provided to rail carriers, in response to feedback from those carriers. We will continue to assess TSA's efforts related to security information-sharing and will report the final results later this year.

Chairman Rockefeller, Ranking Member Hutchison, and members of the Committee, this completes my prepared statement. I look forward to responding to any questions you may have.

GAO Contact and Staff Acknowledgments

For further information on this testimony, please contact Steve Lord at (202) 512-8777 or at lords@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Individuals making key contributions to this testimony include Jessica Lucas-Judy, Assistant Director; Robert Rivas, analyst-in-charge; Charles Bausell; Orlando Copeland; Chris Ferencik; Kevin Heinz; Dawn Hoff; Tracey King; Daniel Klabunde; Stan Kostyla; Landis Lindsey; Ying Long; Robert Lowthian; Marvin McGill; Lauren Membreno; Jessica Orr; and Michael Silver.

Related GAO Products

Public Transit Security Information Sharing: DHS Could Improve Information Sharing through Streamlining and Increased Outreach. GAO-10-895. Washington, D.C.: September 22, 2010.

Technology Assessment: Explosives Detection Technologies to Protect Passenger Rail. GAO-10-898. Washington, D.C.: July 28, 2010.

Surface Transportation Security: TSA Has Taken Actions to Manage Risk, Improve Coordination, and Measure Performance, but Additional Actions Would Enhance Its Efforts. GAO-10-650T. Washington, D.C.: April 21, 2010.

Transportation Security: Key Actions Have Been Taken to Enhance Mass Transit and Passenger Rail Security, but Opportunities Exist to Strengthen Federal Strategy and Programs. GAO-09-678. Washington, D.C.: June 24, 2009.

Transit Security Grant Program: DHS Allocates Grants Based on Risk, but Its Risk Methodology, Management Controls, and Grant Oversight Can Be Strengthened. GAO-09-491. Washington, D.C.: June 8, 2009.

Freight Rail Security: Actions Have Been Taken to Enhance Security, but the Federal Strategy Can Be Strengthened and Security Efforts Better Monitored. GAO-09-243. Washington, D.C.: April 21, 2009.

Transportation Security: Comprehensive Risk Assessments and Stronger Internal Controls Needed to Help Inform TSA Resource Allocation. GAO-09-492. Washington, D.C.: March 27, 2009.

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 afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

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

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548