GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

May 27, 2010

The Honorable John L. Mica
Ranking Member
Committee on Transportation and Infrastructure
House of Representatives

Subject: *Transportation Security: Additional Actions Could Strengthen the Security of Intermodal Transportation Facilities*

Dear Mr. Mica,

Terrorist attacks on mass transit and commuter rail facilities in Moscow, Madrid, London, and Mumbai,[1] and the significant loss of life and disruption they caused, have highlighted the vulnerability of transportation facilities to terrorism and the need for greater focus on securing these facilities, including intermodal transportation terminals.[2] Such intermodal transportation terminals—locations where multiple modes or types of passengers or cargo transportation connect and merge—are potentially high value targets for terrorists because the large number of passengers or volume of cargo can lead to significant loss of human life and economic disruption.[3] For example, New York City's Pennsylvania ("Penn") Station, the nation's busiest rail station, functions as an intermodal hub for Amtrak, two major commuter rail lines (New Jersey Transit and the Long Island Rail Road), as well as six city subway routes. According to Amtrak, an average of 500,000 passengers use the station daily.

[1]The Moscow subway attack occurred on March 29, 2010; the Madrid attack occurred on March 11, 2004; the London attack on July 7, 2005; and the attack in Mumbai on July 11, 2006. Each attack resulted in at least dozens of deaths and injuries.

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

[3]Intermodal transportation terminals are facilities into which multiple transportation modes deliver passengers or cargo, sometimes as the end point of a journey, but also as a transfer point to another transportation mode to continue travel. For example, Amtrak rail stations in large cities are intermodal facilities which serve large numbers of passengers traveling across intersecting modes, such as mass transit (e.g., subway and bus) and passenger rail. Almost all passenger airports and their terminals are inherently intermodal, since most permit passengers to access the terminal building by other vehicles, including buses and taxis, while also serving as the facility to enter the aviation system. Some airport terminals, such as Atlanta's Hartsfield-Jackson, are also internal transfer points to local or regional passenger rail systems, while others, such as Washington, D.C., Reagan National, have subways that adjoin the terminal area, but do not enter it.

The Department of Homeland Security (DHS) has primary responsibility for homeland security, including transportation security, under the Homeland Security Act.[4] Within DHS, the Transportation Security Administration (TSA) has primary responsibility for securing the aviation and surface transportation sectors.[5] The Department of Transportation (DOT) supports DHS by providing technical assistance through some programs (e.g., supporting the development of security standards for mass transit and passenger rail systems). DOT also assists DHS when possible with implementation of its security policies, as allowed by DOT statutory authorities and available resources. A number of other entities, including Amtrak, transportation agencies, local law enforcement, and state and local governments, have day-to-day responsibilities for securing the aviation and surface transportation sectors. Amtrak, for example, operates the nation's primary intercity passenger rail system and serves more than 500 stations across the country. DHS and DOT formalized their roles and responsibilities for transportation security through a memorandum of understanding signed in September 2004, which identified that they would work together to achieve the required level of multi- and intermodal security.[6]

You raised questions about the level of security and protection at intermodal transportation facilities throughout the nation, and asked us to examine federal efforts to secure these facilities. On January 7, 2010, we met with your staff to update them on the status of our work assessing the security of aviation and surface transportation modes and intermodal facilities. As agreed, this report summarizes the work that we have completed in recent years in the aviation and surface transportation security area that is most directly related to intermodal facilities, as well as our ongoing work in these areas.[7] Although this work focused on individual modes and related facilities within the transportation sector—such as aviation, mass transit and passenger rail, freight rail, and highway infrastructure—many of the

[4]Pub. L. No. 107-296, 116 Stat. 2135 (2002). See enclosure I for a list of abbreviations used in this report.

[5]Pub. L. No. 107-71,115 Stat. 597 (2001). For the purposes of this report, we define surface transportation to include mass transit and passenger rail, freight rail, highway infrastructure (including commercial vehicles), and pipelines.

[6]See 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) for examples of collaboration between TSA and the Federal Transit Administration (FTA), which is 1 of 11operating administrations within DOT. Some examples of collaboration include their establishment of working groups composed of federal and industry mass transit and passenger rail security stakeholders to serve as a modal coordinating council for rail systems and their co-hosting of semiannual transit security roundtables, which serve as a means for representatives of the nation's 50 largest mass transit agencies to share security-related ideas and information.

[7]We define work as recently completed if products were issued since January 1, 2008. This report discusses separate, ongoing engagements on the Transportation Worker Identification Credential program and pipeline security (both conducted at the request of the Senate Committee on Commerce, Science, and Transportation).

facilities examined were also intermodal.[8] Thus, this report addresses the following questions:

- To what extent has DHS taken actions to ensure that efforts to strengthen the security of the aviation and surface transportation sectors are based on a risk management framework, particularly those that include intermodal facilities?
- To what extent has DHS taken actions to ensure the security of the aviation and surface transportation sectors, particularly those actions that involve intermodal facilities?

To perform our work, we reviewed relevant reports and documents from TSA, DOT, and Amtrak, including DHS's 2009 National Infrastructure Protection Plan (NIPP),[9] and TSA's May 2007 Transportation Systems Sector-Specific Plan (TSSP),[10] as well as legislation relevant to transportation security, such as the Implementing Recommendations of the 9/11 Commission Act of 2007.[11] We interviewed officials from TSA, DOT, and Amtrak, and subject matter experts at the National Academy of Sciences to discuss the security of intermodal transportation facilities. In addition, we reviewed our recently completed and ongoing work on transportation security across aviation and surface transportation modes and facilities.[12]

We identified our work with a nexus to intermodal security. Therefore, the recent and ongoing work cited in this report does not include all our work related to aviation and surface transportation security, but rather efforts that are germane to intermodal security, and particularly those that assessed the security of intermodal transportation facilities within the United States. We conducted our work from

---

[8]Maritime security is outside the scope of this report. For a summary of GAO's work on maritime security, including security at ports and other intermodal facilities, see *Maritime Security: National Strategy and Supporting Plans Were Generally Well-Developed and Are Being Implemented*, GAO-08-672 (Washington, D.C.: June 20, 2008); *Maritime Security: The SAFE Port Act: Status and Implementation One Year Later*, GAO-08-126T (Washington, D.C.: Oct. 30, 2007); and pages 105-124 of *Department of Homeland Security: Progress Report on Implementation of Mission and Management Functions*, GAO-07-454 (Washington, D.C.: Aug. 17, 2007).

[9]The NIPP established a risk management framework for setting national priorities, goals, and requirements for Critical Infrastructure and Key Resources protection to help ensure that federal funding and resources are applied in the most effective manner. Critical Infrastructure and Key Resources include the assets, systems, networks, and functions that provide vital services to the nation and are dispersed among the following 18 sectors: agriculture and food; banking and finance; chemical; commercial facilities; communications; critical manufacturing; dams, defense industrial base; emergency services; energy; government facilities; healthcare and public health; information technology; national monuments and icons; nuclear reactors, materials, and waste; postal and shipping; transportation systems; and water. See DHS, *National Infrastructure Protection Plan* (Washington, D.C.: 2009). The 2009 NIPP replaced the 2007/2008 and 2006 versions.

[10]The TSSP documents TSA's risk management process to be used in carrying out the strategic priorities outlined in the NIPP and contains supporting implementation plans for each transportation mode. TSA, *Transportation Systems Sector-Specific Plan* (Washington, D.C.: May 2007).

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

[12]The work conducted for those products was done in accordance with generally accepted government auditing standards. For issued reports related to transportation security that we reviewed for this report, see the related products list at the end of the report.

October 2009 through May 2010 in accordance with all sections of GAO's Quality Assurance Framework that are relevant to our objectives. The framework requires that we plan and perform the engagement to obtain sufficient and appropriate evidence to meet our stated objectives and to discuss any limitations in our work. We believe that the information and data obtained and the analysis conducted provide a reasonable basis for any findings and conclusions in this product.

Results in Brief

Although TSA has taken some actions to strengthen the security of aviation and surface transportation facilities through a risk management framework, it has not fully implemented such a framework to inform the allocation of security resources across the transportation modes, including the security of intermodal facilities. For example, we reported in March 2009 that while TSA's transportation sector security plan outlines the need to identify and understand the risk factors associated with intermodal transportation, TSA has not conducted comprehensive risk assessments for the aviation and surface transportation sectors. We recommended that TSA conduct such assessments, which combine information on the three components of risk—threat, vulnerability, and consequence—to help TSA produce a comparative analysis of risk across the transportation sector to guide current and future investment decisions. DHS and TSA concurred with our recommendation and have indicated that they are taking steps to address it.

DHS and its component agencies have taken a number of actions in recent years to help ensure the security of the nation's aviation and surface transportation sectors, including intermodal facilities; however, opportunities exist to strengthen activities related to:

- *personnel*—including workforce planning and training of workers carrying out security activities;
- *operational and management processes*—including coordination among key stakeholders and entities responsible for transportation security; and
- *security and related technologies*—the technical systems and technologies developed and deployed for carrying out these programs.

For example, in terms of personnel, TSA has periodically deployed Visible Intermodal Prevention and Response (VIPR) security teams within mass transit and passenger rail facilities to augment local security forces, but could do more to measure their performance. In our review of the VIPR program's proposed fiscal year 2010 budget, we reported that performance measures had not been fully established to assess the results of VIPR deployments. TSA agreed that performance measures needed to be developed for VIPR teams to measure results, and said that TSA intended to incorporate such metrics.[13] With regard to operational and management processes,

[13]Since late 2005, TSA has deployed VIPR teams consisting of various TSA personnel to augment the security of mass transit and passenger rail systems and promote the visibility of TSA. Working alongside local security and law enforcement officials, VIPR teams conduct a variety of security tactics to introduce unpredictability and deter potential terrorist actions, including random high visibility patrols at mass transit and passenger rail stations and conducting passenger and baggage screening operations using specially trained behavior detection officers and a varying combination of explosive detection canine teams and explosives detection technology.

we reported that while TSA has made progress in a variety of areas related to program implementation across a wide range of transportation security programs, such as conducting assessments to guide investment of security resources and supporting the establishment of information-sharing entities, it continues to face challenges with regard to planning and management of some programs and coordinating with stakeholders. For example, we reported on continuing challenges in implementing the use of the terrorist watchlist to screen individuals and determine if they pose a threat to aviation security and, in a separate report, that key DHS entities were not coordinating their risk assessment activities or sharing results. DHS has since indicated that it is taking steps to address these issues. In terms of technology, we reported in October 2009 that TSA was not fully testing certain airport checkpoint screening equipment in an operational environment prior to deployment.[14] We recommended that, to the extent feasible, TSA ensure that technologies have completed operational tests and evaluations before they are deployed. Although DHS concurred with the recommendation, we disagreed as to whether their proposed actions to address it were sufficient. In March 2010, we reported that although TSA does not yet have a written policy requiring operational testing prior to deployment, a senior TSA official stated that TSA has made efforts to strengthen its operational test and evaluation process and that TSA is now complying with DHS's acquisition directive that requires operational testing and evaluation be completed prior to deployment.[15]

DHS and Amtrak generally concurred with the information presented in the report and DOT did not have any comments.

Background

Since it is neither practical nor 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. 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 June 2006, DHS issued the NIPP, which named TSA as the primary federal agency responsible for coordinating critical infrastructure protection efforts within the transportation sector. The NIPP also 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 effective manner to deter threats, reduce vulnerabilities, and minimize the consequences of attacks and other incidents. The NIPP defines risk as a function of threat, vulnerability, and consequence. Threat is an indication of the likelihood that a specific type of attack will be initiated against a

[14]GAO, *Aviation Security: DHS and TSA Have Researched, Developed, and Begun Deploying Passenger Checkpoint Screening Technologies, but Continue to Face Challenges*, GAO-10-128 (Washington, D.C.: October 2009).

[15]GAO, *Aviation Security: TSA is Increasing Procurement and Deployment of the Advanced Imaging Technology, but Challenges to This Effort and Other Areas of Aviation Security Remain*, GAO-10-484T (Washington, D.C., March 17, 2010).

specific target or class of targets. Vulnerability is the probability that a particular attempted attack will succeed against a particular target or class of targets. Consequence is the effect of a successful attack. An updated version of the NIPP was issued in 2009.

In May 2007, TSA issued the Transportation Systems Sector-Specific Plan (TSSP), which documents the risk management process to be used in carrying out the strategic priorities outlined in the NIPP, and contains supporting implementation plans for each of six major national transportation modes—defined in the TSSP as: aviation; maritime; mass transit (including transit buses, subway and light rail, and passenger rail---both commuter rail and long-distance); highway; freight rail; and pipeline. The TSSP notes the inherent vulnerability of surface transportation, the constant evolution of transportation security, and an increasing dependency on intermodal and international transportation as features of the transportation sector. It further notes that holistic intermodal security planning across all transportation modes is required by the trends of increased volume in international passenger traffic and the expansion of commerce both domestically and globally.

TSA Has Taken Some Actions to Implement a Risk Management Approach but Could Do More to Inform the Allocation of Resources across the Aviation and Surface Transportation Sectors

TSA has taken some actions to implement a risk management approach, but it has not fully implemented a comprehensive risk management approach across the five major transportation modes included in the TSSP aviation and surface transportation sectors, including intermodal facilities.[16] A comprehensive approach would assess threat, vulnerability, and consequence to inform the allocation of resources, as called for by the NIPP and the TSSP. In 2007, TSA initiated but later discontinued an effort to conduct a comprehensive risk assessment for the entire transportation sector, known as the National Transportation Sector Risk Analysis. Specifically, TSA was planning to estimate the threat, vulnerability, and consequence of a range of hypothetical attack scenarios and integrate these estimates to produce risk scores for each scenario that could be compared among each of the modes of transportation. However, officials stated that TSA discontinued its work on the National Transportation Sector Risk Analysis due to difficulties in estimating the likelihood of terrorist threats.

In March 2009, we reported that TSA has taken some actions required by the NIPP's six-step risk management process, but that it has not conducted comprehensive risk assessments across the five major aviation and surface transportation modes

[16]As noted, the sixth transportation mode cited in the TSSP—maritime—is outside the scope of this report.

(aviation, mass transit and passenger rail, freight rail, highway, and pipeline).[17] While TSA had conducted assessments of threat, vulnerability, and consequence within the transportation modes, it had not conducted risk assessments that integrate these three components for each mode or the transportation sector as a whole. We also reviewed 19 assessment activities conducted by DHS and TSA across the five major aviation and surface transportation modes. These reviews included, for example, TSA's Current Airports Threat Assessment, which provides periodic threat information on the nation's airports; the annual threat assessments issued for each of the transportation modes; and other transportation security-related assessment activities, such as TSA's Baseline Assessment and Security Enhancement (BASE) reviews, which evaluate transit systems' implementation of security action items jointly developed by TSA and the FTA.[18] While these 19 assessment activities were not necessarily designed to provide risk information on all three components of risk, 8 provided information on threat, 11 on vulnerability, and 2 on consequence. However, a risk assessment, as required by the NIPP, involves assessing each of the three elements of risk and then combining them together into a single analysis.[19]

---

[17]GAO, *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). The report did not assess risk assessments in the maritime transportation mode; it addressed the five modes of the transportation sector that TSA is responsible for securing: aviation, freight rail, highway infrastructure, mass transit, and pipeline. The six steps specified by the NIPP are: (1) Set security goals: Define specific outcomes, conditions, end points, or performance targets that collectively constitute an effective protective posture; (2) Identify assets, systems, networks, and functions: Develop an inventory of the assets, systems, and networks that comprise the nation's critical infrastructure, key resources, and critical functions, and collect information pertinent to risk management that takes into account the fundamental characteristics of each sector; (3) Assess risks: Determine risk by combining general or specific threat information, known vulnerabilities to various potential attack vectors, potential direct and indirect consequences of a terrorist attack or other hazards; (4) Prioritize: Aggregate and analyze risk assessment results to develop a comprehensive picture of asset, system, and network risk; establish priorities informed by risk; and determine protection and business continuity initiatives that provide the greatest mitigation of risk; (5) Implement protective programs: Select sector-appropriate protective actions or programs to reduce or manage the risk identified and secure the resources needed to address priorities; and (6) Measure effectiveness: Use metrics and other evaluation procedures at the national and sector levels to measure progress and assess the effectiveness of the national protection program in improving protection, managing risk, and increasing resiliency.

[18]For example, the Aviation Mode Annual Threat Assessment provides in-depth analysis of potential threats, while the air cargo vulnerability assessments collect information on how air carriers, freight forwarders, and agents operate their businesses and on physical surroundings, such as the quality of door locks and alarms. Similarly, the rail corridor reviews determine the vulnerabilities and potential consequences that toxic inhalation hazard (TIH) cars pose in major areas by identifying locations within a city's rail network where TIH cars are vulnerable to attack. See GAO-09-492, appendix II, for further details on each of the 19 assessment activities that we evaluated.

[19]See GAO-09-492. In a related June 2009 report, we found that DHS allocates transportation security-related grants based on risk but could improve its risk methodology and grant oversight. See 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 8, 2009). We made seven recommendations to DHS to help strengthen the implementation and oversight of the Transit Security Grant Program; the first specifically recommended that to strengthen its methodology for determining risk, DHS develop a cost-effective method for incorporating vulnerability information into future iterations of the Transit Security Grant Program risk model. DHS concurred with all of the recommendations. In November 2009, DHS updated the status of its efforts,

We recommended that TSA conduct risk assessments that combine threat, vulnerability, and consequence to help the agency produce a comparative analysis of risk across the entire transportation sector, which the agency could use to guide current and future investment decisions. In commenting on our report, DHS and TSA concurred with our recommendation, and TSA identified actions planned, such as integrating the results of risk assessments into a comparative risk analysis across the transportation sector. TSA officials stated in April 2010 that the agency has completed revised versions of its risk management framework, TSSP, and modal annexes. They added that these documents are undergoing final agency review.

In addition to the lack of a comprehensive risk assessment for the nation's aviation and surface transportation sectors, there are also gaps in risk assessments by DHS and TSA for some of the individual transportation modes, including at intermodal facilities within each of them. The following summarizes our findings with regard to these modes for those reports that were relevant to, or included discussions of, intermodal transportation facilities.

Aviation Security

- In September 2009, we reported that while TSA has implemented activities to assess risks to airport perimeters and access controls, such as conducting a commercial aviation threat assessment, it had not conducted vulnerability assessments for 87 percent of the nation's approximately 450 commercial airports or any consequence assessments. As a result, TSA had not completed a comprehensive risk assessment of airports—which are often intermodal facilities—that combines threat, vulnerability, and consequence assessments. With regard to airport security, we noted that TSA's efforts needed to be more consistently guided by a unifying national strategy that identifies key elements, such as priorities and required resources.[20] We recommended that TSA develop a comprehensive risk assessment of airport security. DHS concurred with this recommendation and noted that TSA planned to implement the recommendation through its ongoing efforts to conduct a comprehensive risk assessment for the transportation sector. TSA expects to complete this assessment later this year.

- With regard to airport passenger checkpoint screening technologies, we reported in October 2009 that while TSA had completed a strategic plan in August 2008 to guide research, development, and deployment of such technologies, the plan was not based on an assessment of threat, vulnerability, and consequence.[21] Further, TSA's strategy did not incorporate other key risk management principles—for example, a cost-benefit analysis and performance

---

including that it would continue incorporating agency asset and vulnerability information in a cost-effective manner. We will continue to monitor DHS's progress in addressing this recommendation.

[20]GAO, *Aviation Security: A National Strategy and Other Actions Would Strengthen TSA's Efforts to Secure Commercial Airport Perimeters and Access Controls*, GAO-09-399 (Washington, D.C.: September 30, 2009).

[21]See GAO-10-128.

measures—as set forth in the NIPP. We recommended that after conducting a comprehensive risk assessment and completing cost-benefit analyses and quantifiable performance measures for the passenger screening program, DHS incorporate the results of these efforts into the passenger screening program strategic plan as appropriate. DHS concurred with our recommendation. As noted above, TSA officials said that they are in the process of updating the TSSP.

Mass Transit and Passenger Rail Security

- 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, combining threat, vulnerability, and consequence.[22] Specifically, DHS had developed a Strategic Homeland Infrastructure Risk Assessment framework that assessed risk across 18 critical infrastructure and key resource sectors. To develop this risk assessment framework, DHS collaborated with members of the intelligence community to determine threats against various systems and assets in the 18 sectors.[23] TSA then assessed the vulnerabilities and consequences that resulted from these threat scenarios and provided this information to DHS's Homeland Infrastructure Threat Reporting and Analysis Center. However, TSA officials stated that the threat scenarios provided to DHS were general and not specific to mass transit and passenger rail. In contrast, we reported that Amtrak has reported conducting risk assessments that incorporate and combine all three risk elements for all of its rail networks.[24] We recommended that TSA, as the lead federal agency for mass transit and passenger rail, conduct a risk assessment that integrates all three elements of risk. DHS concurred with the recommendation, and in April 2010, DHS officials said that TSA had undertaken a Transportation Systems Sector Risk Assessment that would incorporate all three elements of risk, and anticipated reporting the results to the appropriate congressional committees in 2010.

Freight Rail Security

- In April 2009, we reported that TSA's efforts with regard to assessing security threats to freight rail could be strengthened.[25] Specifically, we noted that

[22]See GAO-09-678.

[23]The 18 industry sectors include agriculture and food, banking and finance, chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, government facilities, information technology, national monuments and icons, nuclear, postal and shipping, public health and healthcare, transportation, and water. For further details and discussion, see GAO-09-678.

[24]According to Amtrak, some of these initial risk assessments were funded by TSA through the Transit Security Grant Program.

[25]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).

while TSA had developed a security strategy, its efforts had focused almost exclusively on rail shipments of toxic inhalation hazards (TIH), which can be fatal if inhaled, while other federal and industry assessments have identified additional potential security threats, including risks to critical infrastructure, such as bridges, tunnels, and control centers.[26] 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. However, we reported that there are other security threats for TSA to consider and evaluate as its freight rail strategy matures, such as potential sabotage to critical infrastructure. We recommended that TSA expand its efforts to include all security threats in its freight rail security strategy. DHS concurred. Since we issued our report, DHS reported that TSA has developed a Critical Infrastructure Risk Tool for measuring the criticality and vulnerability of freight railroad bridges and used it to assess 39 railroad bridges, with plans to assess an additional 22 by the end of 2010. We will continue to monitor TSA's progress in addressing this recommendation.

[26]TIH materials include chlorine (used in water treatment) and anhydrous ammonia (used in agriculture). In addition, shipments of TIH, especially chlorine, frequently move through densely populated areas to reach, for example, water treatment facilities that use these products.

- Securing the nation's highway infrastructure system is a responsibility shared by federal, state and local governments, and the private sector, including major associations representing highway owners and operators. The federal government is also responsible for providing some funding assistance to highway infrastructure stakeholders. In January 2009, we reported that although DHS entities have several programs underway to conduct threat, vulnerability, and consequence assessments of highway infrastructure assets, the scope and purpose of these individual efforts varied considerably, were at various levels of completion, were not systematically coordinated, and the results had not been routinely shared among the entities or with another key stakeholder, the Federal Highway Administration.[27] TSA has used these assessments to assess the general state of security for the sector, and to identify potential security enhancements for a majority of highway infrastructure assets identified as nationally critical. However, without adequate coordination with federal partners, we reported that TSA was unable to determine the extent to which specific critical assets had been assessed and whether potential adjustments in its methodology were necessary to target remaining critical infrastructure assets. We recommended that to enhance collaboration among entities involved in securing highway infrastructure and to better leverage federal resources, DHS establish a mechanism to systematically coordinate risk assessment activities and share the results of these activities among the federal partners. DHS concurred with the recommendation, and stated that TSA would take the lead in developing a sector coordinated risk assessment.

- In addition, in commenting on a draft of that January 2009 report, TSA stated that it recognized that it is responsible for all non-maritime transportation security matters, intends to fulfill its leadership role in the highway infrastructure arena, and was prepared to assume responsibility for all highway infrastructure security issues.[28] In February 2010, TSA reported that it had taken various actions to address the recommendation.[29] Specifically, TSA stated that its Highway and Motor Carrier Division had initiated an interagency agreement with the U.S. Army Corps of Engineers to conduct on-site highway infrastructure assessments. TSA further stated that it had met with all federal agencies currently known to conduct security reviews of highway structures to: (1) identify existing data resources; (2) establish a data sharing system among key agencies; and (3) propose that standards be established and agreed upon by all participating agencies for collecting data for and conducting and sharing data for any future assessment. According to

[27]GAO, *Highway Infrastructure: Federal Efforts to Strengthen Security Should Be Better Coordinated and Targeted on the Nation's Most Critical Highway Infrastructure*, GAO-09-57 (Washington, D.C.: Jan. 30, 2009). The bulk of the responsibility for implementing specific security measures falls largely on state and local governments who own most highway infrastructure.

[28]See GAO-09-57.

[29]TSA: *February 2010 Updates to GAO-09-57*. GAO has not yet reviewed or evaluated TSA's actions to address the recommendation.

TSA, those discussions resulted in agreement by all interested agencies (within DHS and DOT) that the U.S. Army Corps of Engineers' work would meet the assessment needs of all involved agencies by following protocols and incorporating methodologies agreed upon by all parties.

Pipeline Security

- Pipelines can also be intermodal, such as when they transport fuel to airports. We are currently conducting an assessment of TSA's efforts to help ensure pipeline security. Among other things, we are evaluating the extent to which TSA's Pipeline Security Division has used a risk management approach to help strengthen the security of these pipelines. As we reported in April 2010, our preliminary observations found that TSA has identified the 100 most critical pipeline systems in the United States and produced a pipeline risk assessment model, consistent with the NIPP.[30] Furthermore, the 9/11 Commission Act requires that risk assessment methodologies be used to prioritize actions to the highest risk pipeline assets, and we found that TSA's stated policy is to consider risk when scheduling Corporate Security Reviews—assessments of pipeline operators' security plans. However, we found a weak statistical correlation between a pipeline system's risk rank and the time elapsed between a first and subsequent review.[31] In addition, we found that among the 15 highest risk-ranked pipeline systems, the time between a first and second Corporate Security Review ranged from 1 to 6 years as of April 2010, and two of these had not had a second review in more than 6 years. TSA Pipeline Security Division Officials told us that although a pipeline system's relative risk ranking is the primary factor driving their decision of when to schedule a subsequent review, they also considered other factors. These included geographical proximity to reduce travel time and costs, and the extent they had worked with the operators through other efforts, such as their Critical Facility Inspection Program.[32] Better prioritizing its reviews based on risk could help TSA ensure its resources are more efficiently allocated toward the highest-risk pipeline systems. We expect to issue a report on the results of this effort by the end of 2010.

[30]GAO, *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).

[31]We calculated a simple correlation coefficient to measure the strength and direction of the linear relationship between systems' risk rankings and the time elapsed between TSA's first and subsequent Corporate Security Reviews for pipeline systems. The magnitude of the correlation coefficient determines the strength of the correlation. Our preliminary analysis resulted in a weak correlation coefficient score.

[32]The Pipeline Security Division established a Critical Facility Inspection Program in November 2008. The program involves on-site physical security inspections of each critical facility of the 100 most critical pipeline systems.

DHS Has Taken Steps to Ensure the Security of Aviation and Surface Transportation Intermodal Facilities, but Could Further Strengthen Its Efforts

In recent years, we have reported that DHS and TSA have taken a number of actions to bolster aviation and surface transportation security, including the security of intermodal transportation facilities. These actions have generally fallen into three broad categories—personnel (including workforce planning and personnel training); operational and management processes (including implementation of security related programs, performance metrics and monitoring, and coordination among stakeholders); and technology (development and utilization of technologies intended to identify security threats). However, as we have reported, many challenges remain to meet NIPP and TSSP goals in several transportation modes, including their intermodal facilities.

TSA Has Made Progress in Workforce Planning and Training Personnel, but Improvements in Management of Personnel Issues Could Further Strengthen the Security of Intermodal Facilities

In our reviews of personnel issues related to aviation and surface transportation security—including TSA's VIPR teams that are periodically deployed to protect intermodal facilities such as airports and rail stations—we reported that TSA had made progress in workforce planning for programs required to enhance security but that training and assessment of workplace performance continue to provide challenges that need to be addressed. The following summarizes findings related to intermodal transportation and the intermodal facilities included therein.

Aviation Security

- We reported in April 2008 that TSA had hired and deployed a federal workforce of over 50,000 passenger and checked baggage screeners, at over 400 commercial airports, and had developed standards for determining screener staffing levels at airports.[33] We also reported that TSA had made progress in training aviation security personnel, many of whom work at airports that are intermodal facilities. These efforts included providing enhanced explosives-detection and recurrent (ongoing) training for all Transportation Security Officers (TSO), who carry out screening of passengers and their hand baggage at airports. In addition, we reported that TSA had trained and deployed federal air marshals on high-risk flights and established standards for training flight and cabin crews, among other things.[34]

[33]GAO, *Transportation Security: Efforts to Strengthen Aviation and Surface Transportation Security Continue to Progress, but More Work Remains*, GAO-08-651T (Washington, D.C.: April 15, 2008).

[34]This progress was built upon earlier steps DHS and TSA had taken to strengthen the management and performance of the TSO workforce by, for example, developing and implementing a Staffing Allocation Model to determine TSO staffing levels at airports that reflected current operating conditions; implementing a variety of human capital initiatives to help recruit, hire, and retain TSOs (both full-time and part-time); and providing TSOs with additional training intended to enhance the detection of threat objects, particularly improvised explosive devices. See GAO, *Aviation Security: Progress Made in Systematic Planning to Guide Key Investment Decisions, but More Work Remains*, GAO-07-448T

- In April 2007, TSA redesigned their local covert testing program to establish the Aviation Screening Assessment Program , intended to test the performance of the passenger and checked baggage screening systems, to include the TSO workforce. We reported in August 2008 that it was too soon to determine at that time whether the program would meet its goals of identifying vulnerabilities and measuring the performance of passenger and checked baggage screening.[35] According to TSA, the program remains in place, and is in use at airports throughout the country.

Mass Transit and Passenger Rail Security

- We reported in June 2009 that TSA had taken a number of actions to secure mass transit and passenger rail systems, such as deploying over 800 VIPR teams to augment mass transit and passenger rail systems' security forces to conduct random and event-based security operations.[36] The VIPR program is intermodal in that its operations augment security at key intermodal transportation facilities, such as Amtrak rail stations. However, questions have been raised about the effectiveness of the VIPR program. In June 2008, for example, the DHS Office of Inspector General reported that although TSA had made progress in addressing problems with early VIPR deployments, it needed to develop a more collaborative relationship with local transit officials if VIPR exercises were to enhance mass transit security.[37] In our review of the VIPR program's proposed fiscal year 2010 budget, we further reported that performance measures had not been fully established to assess the results of VIPR deployments. TSA agreed that performance measures needed to be developed for VIPR teams, and said that TSA intended to incorporate such metrics, including for measuring interagency collaboration and stakeholder views on the effectiveness of VIPR deployment, in fiscal year 2010.

(Washington, D.C.: Feb. 13, 2007). See also the GAO report on which the Feb. 2007 testimony was based, GAO, *Aviation Security: TSA's Staffing Allocation Model Is Useful for Allocating Staff among Airports, but Its Assumptions Should Be Systematically Reassessed*, GAO-07-299 (Washington, D.C.: Feb. 28, 2007).

[35]GAO, *Transportation Security: TSA Has Developed a Risk-Based Covert Testing Program, but Could Better Mitigate Aviation Security Vulnerabilities Identified Through Covert Tests*, GAO-08-958 (Washington, D.C.: August 8, 2008). We have not subsequently assessed the performance of the ASAP program. However, we will continue to monitor TSA's progress in addressing our related recommendation. For other work we did on airport worker screening issues, see GAO-09-399.

[36]See GAO-09-678 for more information on TSA's VIPR program. VIPR missions are deployments of integrated TSA and other federal, state, or local personnel to secure any mode of transportation. VIPR teams employ a variety of tactics to deter terrorism, including performing random high visibility patrols at mass transit stations, conducting passenger and baggage screening operations, using behavior detection officers, and deploying canine detection teams and explosive detection technologies. According to Amtrak, Amtrak and TSA have conducted over 300 VIPR operations across the Amtrak route system since 2007.

[37]Department of Homeland Security, Office of Inspector General, *TSA's Administration and Coordination of Mass Transit Security Programs*, OIG-08-66 (Washington, D.C.: June 12, 2008).

- Over the last 2 years, TSA has more than doubled the size of its Surface Transportation Security Inspection Program, expanding the program from 93 inspectors in June 2008 to 201 inspectors in April 2010.[38] As of April 2010, TSA's surface inspectors had conducted security assessments of 142 mass transit and passenger rail agencies, and had conducted over 1,350 site visits to mass transit and passenger rail stations to complete station profiles, which gather detailed information on a station's physical security elements, geography, and emergency points of contact.[39] However, we reported in June 2009 that TSA did not have a human capital or other workforce plan for its Surface Transportation Security Inspection Program, but that the agency had plans to conduct a staffing study to identify the optimal workforce size to address its current and future program needs.[40] We noted that TSA reported that it had initiated a study in January 2009 to be completed in late fiscal year 2009, which, if completed, could provide TSA with a more reasonable basis for determining the surface inspector workforce needed to achieve its current and future workload needs. In March 2010, TSA officials told us that while they were continuing to work on a staffing study, TSA did not have a firm date for completion.

- In June 2009, we reported that TSA had established the Mass Transit Security Training Program in February 2007 to provide transit agencies with curriculum guidance and expedited grant funding to cover training costs for frontline employees, including those protecting intermodal facilities. However, 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. 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.[41] DHS concurred with the recommendation, noting

[38]TSA intends to hire an additional 179 surface inspectors in fiscal year 2010. The April 2010 data include headquarters staff.

[39]According to TSA, the Surface Transportation inspectors provide support to the nation's largest mass transit and passenger rail systems, and perform frequent inspections of key facilities including stations and terminals for suspicious or unattended items, among others potential threats. TSA states that the inspectors are actively engaged in performing Security Analysis and Action Programs, which constitute a systematic examination of stakeholder operations to assess compliance with security requirements, identify security gaps, develop best practices, and gather information on the system, its operations, and its security resources and initiatives.

[40]See GAO-09-678.

[41]TSA allows transit systems to obtain DHS grant funding to contract with private security training vendors if TSA has determined that the performance of the vendors' training curriculum and delivery services is equal to those of the federally sponsored providers. DHS must review transit agency applications for nonfederally sponsored or funded training venders and discern the extent to which each vendor it reviews will provide training programs whose curriculum and delivery services generally equal or exceed the performance of those provided by federally sponsored training

that TSA would work with FTA through an existing joint working group to develop criteria for reviewing new vendor-provided training courses.[42] 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. TSA stated that this approach recognizes the experience FTA has gained in sponsoring and coordinating development of safety and security training programs over the course of many years. TSA further stated that its goal is to set objective criteria for each of the course areas listed in training program guidelines it had developed and disseminated to the mass transit and passenger rail community in February 2007.

Federal Agencies Are Conducting Assessments to Guide Investment of Security Resources and Supporting the Establishment of Information-Sharing Entities, but Continue to Face Challenges in Operational and Management Processes

Implementation of programs to strengthen transportation security includes the process of developing and deploying the security programs, and the coordination among stakeholders and relevant agencies that have overlapping responsibilities with regard to ensuring transportation security. The implementation of transportation sector programs includes intermodal facilities such as airports and airport terminals, major rail stations, and highway infrastructure facilities.

Aviation Security

Since its inception in November 2001, TSA has focused much of its efforts on aviation security, and has developed and implemented a variety of programs and procedures to secure the commercial aviation system. TSA has taken steps to strengthen passenger checkpoint screening procedures to enhance the detection of prohibited items, as well as to make checking of passenger names against the terrorist watchlist records more effective in detecting persons who may pose a threat to aviation security. These initiatives have been intended to improve aviation security, including that of airports and their terminals, which are often intermodal in nature. While making progress, TSA and other federal agencies have faced challenges in effectively implementing certain programs integral to ensuring aviation security.

- In July 2008, we reported that DHS and TSA had undertaken numerous initiatives to strengthen the security of the nation's commercial aviation system, including actions to address many recommendations we have made.[43] For example, TSA has taken steps to strengthen passenger checkpoint screening procedures to enhance the detection of prohibited items. TSA focused its efforts on, among other things, more efficiently allocating, deploying, and managing the TSO workforce; strengthening screening

---

providers. At the time of our report, federally sponsored training providers included the National Transit Institute, the Transportation Safety Institute, and Johns Hopkins University.

[42]See GAO-09-678.

[43]GAO, *Aviation Security: Transportation Security Administration Has Strengthened Planning to Guide Investments in Key Aviation Security Programs, but More Work Remains*, GAO-08-1024T (Washington, D.C.: July 24, 2008).

procedures; developing and deploying more effective and efficient screening technologies; strengthening domestic air cargo security. TSA also explored new passenger checkpoint screening technologies to better detect explosives and other threats, and has taken steps to strengthen air cargo security, including increasing compliance inspections of air carriers. At the same time, we reported that several areas that should be addressed to further strengthen security. For example, TSA had made limited progress in developing and deploying checkpoint technologies due to planning and management challenges. (See below for further discussion of these technology-related challenges.)

- In a January 27, 2010 analysis of the attempted bombing on December 25, 2009, of Northwest flight 253, we reported on continuing challenges in implementing the use of the terrorist watchlist to screen individuals and determine if they pose a threat to aviation security, as well as how aspects of this process contributed to the December 25 attempted attack.[44] We reported that because, in part, the alleged attacker was not nominated for inclusion on the government's consolidated terrorist screening database, federal agencies responsible for screening activities missed several opportunities to identify him and possibly take action. We have previously reported on a number of issues related to the compilation and use of watchlist records, such as the potential security risk posed by not checking against all records on the watchlist. We also identified the need for an up-to-date strategy and implementation plan—one that describes the scope, governance, outcomes, milestones, and metrics, among other things—for managing the watchlist process across the federal government. Such a strategy and plan, supported by a clearly defined leadership or governance structure, could be helpful in removing cultural, technological, and other barriers that inhibit the effective use of watchlist information.

  Since fiscal year 2004, GAO has been required to assess the development and implementation of the Secure Flight program, an advanced passenger prescreening program to assume from air carriers the function of matching passenger information against terrorist watchlist records.[45] We have reported on numerous challenges the program has faced, including those related to protecting passenger privacy, completing performance testing, fully defining and testing security requirements, and establishing reliable cost and schedule

[44]GAO, *Homeland Security: Better Use of Terrorist Watchlist Information and Improvements in Deployment of Passenger Screening Checkpoint Technologies Could Further Strengthen Security*, GAO-10-401T (Washington, D.C.: Jan. 27, 2010).

[45]GAO has performed this work in accordance with statutory mandates, beginning in fiscal year 2004 with the Department of Homeland Security Appropriations Act, 2004, Pub. L. No. 108-90, § 519, 117 Stat. 1137, 1155-56 (2003) (establishing the initial mandate that GAO assess the Computer-Assisted Passenger Prescreening System II, the precursor to Secure Flight, and setting forth the original eight statutory conditions related to the development and implementation of the prescreening system), and pursuant to the requests of various congressional committees.

estimates, among other things.[46] We have made recommendations to address these challenges, and TSA has generally agreed with them and has taken corrective actions. Section 522(a) of the Department of Homeland Security Appropriations Act, 2005, set forth 10 conditions related to the development and implementation of the Secure Flight program that the Secretary of Homeland Security must certify have been successfully met before the program may be implemented or deployed on other than a test basis.[47] In May 2009, we reported that TSA had generally achieved 9 of the 10 statutory conditions and had conditionally achieved 1 condition, subject to the timely completion of planned activities for developing appropriate cost and schedule estimates.[48] In April 2010, we reported that TSA has generally achieved the statutory condition related to the appropriateness of Secure Flight's life-cycle cost and schedule estimates, and thus has generally achieved all 10 statutory conditions related to the development and implementation of the program.[49] TSA plans to complete assumption of the watchlist-matching function from air carriers for all domestic flights in May 2010 and to assume this function for all international flights departing to and from the United States by December 2010. If effectively maintained and updated, TSA's cost and schedule estimates should help ensure oversight and accountability of the Secure Flight program and provide assurance that it will be delivered within estimated costs and time frames.

Mass Transit and Passenger Rail Security

- In June 2009, we reported that TSA had taken actions to enhance mass transit and passenger rail system security, such as conducting voluntary security assessments of the nation's largest mass transit and passenger rail systems and establishing the monthly Transit Policing and Security Peer Advisory Group to act as a consultative forum for advancing the security of transit systems.[50] We

---

[46]See, for example, GAO, *Aviation Security: Transportation Security Administration Has Strengthened Planning to Guide Investments in Key Aviation Security Programs, but More Work Remains*, GAO-08-456T (Washington, D.C.: Feb. 28, 2008).

[47]See Pub. L. No. 108-334, § 522, 118 Stat. 1298, 1319-20 (2004). The appropriations acts for each subsequent fiscal year through fiscal year 2009 included the same requirement, referring back to the 10 conditions from fiscal year 2005. See Department of Homeland Security Appropriations Act, 2006, Pub. L. No. 109-90, § 518(a), 119 Stat. 2064, 2085 (2005); Department of Homeland Security Appropriations Act, 2007, Pub. L. No. 109-295, § 514(a), 120 Stat. 1355, 1379 (2006); Consolidated Appropriations Act, 2008, Pub. L. No. 110-161, div. E, § 513(a), 121 Stat. 1844, 2072 (2007); and Consolidated Security, Disaster Assistance, and Continuing Appropriations Act, 2009, Pub. L. No. 110-329, div. D, § 512(a), 122 Stat. 3652, 3682 (2008). The conditions related to, among other things, protecting passenger privacy, completing performance testing, fully defining and testing security requirements, and establishing reliable cost and schedule estimates.

[48]GAO, *Aviation Security: TSA Has Completed Key Activities Associated with Implementing Secure Flight, but Additional Actions Are Needed to Mitigate Risks*, *GAO-09-292* (Washington, D.C.: May 13, 2009).

[49]GAO, *GAO Review of the Department of Homeland Security's Certification of the Secure Flight Program—Cost and Schedule Estimates*, GAO-10-535R (Washington, D.C.: Apr. 5, 2010).

[50]See GAO-09-678. Amtrak also participates in the Peer Advisory Group.

made six recommendations related to improving TSA's approach to the mass transit and rail sector security, including changes to risk assessments and training, and expanding related technology and research efforts. DHS concurred with all six recommendations. In February 2010, DHS stated that it was developing a common (integrated) platform that will enable TSA and its security partners in DHS to conduct joint assessments of mass transit and passenger rail agencies. In April 2010, TSA indicated that this platform was still under development.

Freight Rail Security

- In April 2009, we reported that while federal and industry stakeholders have taken a number of steps to coordinate their freight rail security efforts, such as implementing agreements to clarify roles and responsibilities and participating in various information-sharing entities, federal coordination could be enhanced by more fully leveraging the resources of all relevant federal agencies, such as TSA and DOT's Federal Railroad Administration (FRA).[51] For example, we recommended that DHS work with federal partners such as FRA to ensure that all relevant information, such as threat assessments, is shared. DHS concurred with this recommendation and articulated that it planned to better define stakeholder roles and responsibilities in order to facilitate information sharing. Since we issued our report, DHS reported that TSA continues to share information with security partners, including meeting with FRA and the DHS Office of Infrastructure Protection to discuss coordination and develop strategies for sharing relevant assessment information and avoiding duplication. We will continue to monitor DHS and TSA's progress in addressing this recommendation.

Highway Infrastructure Security

- In January 2009, we reported that while several component agencies within DHS and DOT were conducting individual risk assessment efforts of highway infrastructure vulnerabilities, key DHS entities had reported that they were not coordinating their activities or sharing the results.[52] We noted that coordination of risk assessment activities would help DHS more effectively use scarce resources to target further assessment activities, and we recommended that DHS establish a mechanism to enhance coordination of risk assessments. DHS concurred with the recommendation. Since we issued our report, agency officials told us that TSA and other federal agencies that conduct security reviews of highway structure will be coordinating in a number of areas, including identifying existing data resources; establishing a data sharing system among key agencies; and proposing the establishment of a standard for data collection and sharing related to risk assessments.

[51]See GAO-09-243. We also reported on coordination-related challenges for TSA in October 2009. See GAO-10-128.

[52]See GAO-09-57.

- In February 2009, we reported that TSA had taken actions to improve coordination with federal, state, and industry stakeholders in the surface transportation sector—specifically with regard to commercial vehicles.[53] These actions included signing joint agreements with DOT and supporting the establishment of intergovernmental and industry councils. However, we also reported that more could be done to ensure that these efforts enhance security by more clearly defining stakeholder roles and their responsibilities. For example, one group of state transportation officials stated that they tried to discuss with TSA and DHS what role the states play in transportation security, but neither agency responded by providing fully defined roles or communicating TSA's strategy to secure commercial vehicles. Other state officials said they had to delay implementing their own initiatives pending TSA clarification of state roles and responsibilities. As a result, we recommended that TSA establish a process to strengthen coordination with the commercial vehicle industry, including ensuring that the roles and responsibilities of industry and government are fully defined and clearly communicated; DHS concurred with this recommendation. In April 2010, TSA stated that it has completed revised versions of its risk management framework, the TSSP, and the modal annexes. They added that these documents are undergoing final agency review.

Pipeline Security

- We are currently conducting an assessment of TSA's efforts to help ensure pipeline security. Among other things, we are evaluating the extent to which TSA's Pipeline Security Division has taken actions to implement the requirements of the Implementing Recommendations of the 9/11 Commission Act of 2007 regarding the security of hazardous liquid and natural gas pipeline systems. We expect to issue a report on the results of this effort by the end of 2010.

DHS Continues to Work on Developing Security Technologies, but Challenges Remain

DHS has made progress in the technology area but continues to face challenges in the development and utilization of technologies intended to identify security threats.

Aviation Security

- On March 17, 2010, in an analysis of the December 25, 2009, attempted attack on Northwest flight 253, we reported that while TSA has taken actions towards strengthening other areas of aviation security, it continues to face challenges involving its efforts to procure and deploy advanced imaging technology (AIT)

[53]GAO, *Commercial Vehicle Security: Risk-Based Approach Needed to Secure the Commercial Vehicle Sector*, GAO-09-85 (Washington, D.C.: February 27, 2009). Commercial vehicles refers to those vehicles used in the commercial trucking industry (e.g., for-hire and private trucks moving freight, rental trucks, and trucks carrying hazardous materials) and the commercial motor coach industry (i.e., intercity, tour, and charter buses). For the purposes of this report, we are including them in the highway infrastructure mode.

(formerly called the Whole Body Imager).[54] We found that in response to the attack, TSA had revised the AIT procurement and deployment strategy, increasing the planned deployment of AITs from 878 to 1,800 units and using AITs as a primary—instead of a secondary—screening measure where feasible. While officials said AITs performed as well as physical pat downs in operational tests, it remains unclear whether the AIT would have detected the weapon used in the December 2009 incident based on the preliminary information we have received. We are currently assessing TSA's operational testing of the AIT.

- We reported in October 2009 that since TSA's creation in November 2001, 10 passenger screening technologies have been in various phases of research, development, test and evaluation, procurement, and deployment, but TSA has not deployed any of these technologies to airports nationwide.[55] The explosives trace portal (ETP), the first new technology deployment initiated by TSA, was halted in June 2006 because of performance problems and high installation costs. TSA's acquisition guidance and leading commercial firms recommend testing the operational effectiveness and suitability of technologies or products prior to deploying them. However, in the case of the ETP, although TSA tested earlier models, the models ultimately chosen were not operationally tested before they were deployed to ensure they demonstrated effective performance in an operational environment. We recommended that, to the extent feasible, DHS ensure that technologies have completed operational tests and evaluations before they are deployed. Although DHS concurred, we reported that their proposed actions to address the recommendation were insufficient.[56] In March 2010, we reported that although TSA does not yet have a written policy requiring operational testing prior to deployment, a senior TSA official stated that TSA has made efforts to strengthen its operational test and evaluation process and that TSA is now complying with DHS's acquisition directive that requires operational testing and evaluation be completed prior to deployment.[57]

Mass Transit and Passenger Rail Security

- With regard to progress made to ensure the security of mass transit and passenger rail systems, including their intermodal facilities, we reported in June 2009 that TSA has taken initial actions to share information on available security technologies, but could strengthen its approach by providing more

[54]The AITs produce an image of a passenger's body that TSA personnel use to look for anomalies, such as explosives. TSA is deploying AITs to airport passenger checkpoints to enhance its ability to detect explosive devices and other prohibited items on passengers. See GAO-10-484T.

[55]See GAO-10-128.

[56]DHS commented that TSA had prepared a Test and Evaluation Master Plan that described a new testing process. However, we reported that we had found that the plan did not address the intent of this recommendation; our evaluation of the plan was classified by DHS as sensitive security information and therefore is not provided in this public report.

[57]See GAO-10-484T.

information to support transit agencies that are considering deploying new security technologies.[58] Consistent with a recommendation we made in September 2005, TSA established the Public Transit Portal of DHS's Homeland Security Information Network (HSIN), a secure web site that serves as a clearinghouse of information on available security technologies that have been tested and evaluated by DHS, in addition to providing security alerts, advisories, and information bulletins. In February 2009, TSA reported that it had established HSIN accounts for 75 of the 100 largest mass transit and passenger rail systems. However, officials from 11 of 17 mass transit and passenger rail systems who discussed HSIN told us that they did not use it for guidance on available security technologies when considering security technology investments. TSA stated that its goal for HSIN was to provide a way for transit agencies to share, receive, and find information on security technology as well as to provide a technology database with performance standards and product capabilities so that mass transit and passenger rail agencies would be well prepared to interact with vendors. However, there was no set deadline for the content-related improvements. We noted that by taking action to address mass transit and passenger rail agencies' need for more information, TSA could help provide transit agencies with a consolidated source of information on security technologies and help ensure that limited resources are not used to duplicate research and testing efforts. In late 2009, a DHS official told us that DHS is in the process of taking steps to improve HSIN, including collecting intelligence and content requirements from stakeholders for all 18 critical sectors to boost participation.

Cross-Cutting Security

We reported in November 2009 that more than 1 million workers across multiple transportation modes access secure areas of port facilities each day.[59] These include longshoremen, truck drivers delivering and picking up cargo, mechanics and merchant mariners, and railroad crews of the freight trains that enter port areas. The Transportation Worker Identification Credential (TWIC) program requires workers who seek unescorted access to secure areas of Maritime Transportation Security Act (MTSA)-regulated facilities and mariners holding Coast Guard-issued credentials to complete background checks and obtain an identification card with biometric capabilities.[60] We reported in November 2009 that the pilot program, intended to test whether the biometric identification cards will function as required, and inform the development of the federal regulation on using TWIC card readers, faces unresolved challenges. These challenges include the lack of a standard to assess the business and operational impacts of using TWIC with biometric card readers. To ensure that the information needed to assess the impacts of deploying TWIC biometric card readers at MTSA-regulated facilities is acquired prior to the development of the

[58]See GAO-09-678.

[59]GAO, *Transportation Worker Identification Credential: Progress Made in Enrolling Workers and Activating Credentials but Evaluation Plan Needed to Help Inform the Implementation of Card Readers*, GAO-10-43 (Washington, D.C.: November 18, 2009).

[60]We included the TWIC program in this report because it affects workers in the highway and freight rail modes.

federal regulation, we recommended that TSA identify how it will compensate for areas where the TWIC reader pilot will not provide the necessary information needed to report to Congress and implement the card reader rule. Although DHS concurred with this recommendation, we noted that it was not clear from DHS's comments whether their proposed actions would fully address it. We reported that while TSA had developed a test and evaluation master plan for the TWIC pilot, the document did not identify the business and operational data to be collected during the pilot, or the performance standards and methodology for assessing the data. To meet the intent of our recommendation, this information would need to be included in the evaluation plan prior to proceeding with the pilot. In its response, DHS identified guidance that it plans to use to supplement the data gathered from the pilot. We also have an ongoing review to evaluate the extent to which TWIC program security measures limit access to MTSA-regulated facilities and vessels. We expect to issue a report with the final results later this year.

Agency Comments

We requested comments from the Secretaries of DHS and DOT and the President and Chief Executive Officer of Amtrak. These entities did not provide official written comments to include in the report. However, on May 12, 2010, the DHS liaison stated that DHS generally concurred with the information presented in the report. In an email received May 13, 2010, the DOT liaison said that the Department did not have any comments. In an e-mail received May 11, 2010, the Amtrak liaison stated that Amtrak generally supports our findings that more coordination and effort is needed. The liaison stated that Amtrak believes that intermodal gaps in rail and mass transit security exist and that TSA should be the key agency in addressing intermodal issues, pushing for more collaboration, information sharing, and integration of rail and mass transit security and law enforcement resources at all government and private industry levels. The liaison also stated that Amtrak has worked with TSA on many security-related projects and that TSA has been a partner and advocate for improving rail passenger security at Amtrak. Finally, Amtrak provided technical comments that we have incorporated as appropriate.

DHS also provided a technical comment, which we incorporated as appropriate.

As we agreed with your office, unless you publicly announce its contents earlier, we plan no further distribution of this report until 25 days after its issue date. At that time, we will send copies of this report to the Secretary of Homeland Security, the Secretary of Transportation, the President and Chief Executive Officer of Amtrak, appropriate congressional committees, and other interested parties. This report will also be available at no charge on the GAO Web site at http://www.gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs are listed on the last page of this report.

If you or your staff have any questions regarding this report, please contact me at (202) 512-8777 or at jeszeckc@gao.gov.

Sincerely yours,

Charles Jeszeck
Director, Homeland Security and Justice Issues

Enclosures – 3

Abbreviations

AIT	Advanced Imaging Technology
DHS	Department of Homeland Security
DOT	Department of Transportation
ETP	Explosives Trace Portal
FRA	Federal Railroad Administration
FTA	Federal Transit Administration
HSIN	Homeland Security Information Network
MTSA	Maritime Transportation Security Act
NIPP	National Infrastructure Protection Plan
TIH	Toxic Inhalation Hazards
TSA	Transportation Security Administration
TSSP	Transportation Systems Sector-Specific Plan
TWIC	Transportation Worker Identification Credential
VIPR	Visible Intermodal Prevention and Response

Related GAO Products

Aviation Security

GAO Review of the Department of Homeland Security's Certification of the Secure Flight Program--Cost and Schedule Estimate. GAO-10-535R. Washington, D.C.: Apr. 5, 2010.

Aviation Security: TSA is Increasing Procurement and Deployment of the Advanced Imaging Technology, but Challenges to This Effort and Other Areas of Aviation Security Remain. GAO-10-484T. Washington, D.C.: March 17, 2010.

Homeland Security: Better Use of Terrorist Watchlist Information and Improvements in Deployment of Passenger Screening Checkpoint Technologies Could Further Strengthen Security. GAO-10-401T. Washington, D.C.: January 27, 2010.

Aviation Security: A National Strategy and Other Actions Would Strengthen TSA's Efforts Aviation Security: DHS and TSA Have Researched, Developed, and Begun Deploying Passenger Checkpoint Screening Technologies, but Continue to Face Challenges. GAO-10-128. Washington, D.C.: October 7, 2009.

Aviation Security: A National Strategy and Other Actions Would Strengthen TSA's Efforts to Secure Commercial Airport Perimeters and Access Controls, GAO-09-399. Washington, D.C.: September 30, 2009.

Aviation Security: TSA Has Completed Key Activities Associated with Implementing Secure Flight, but Additional Actions Are Needed to Mitigate Risks. GAO-09-292. Washington, D.C.: May 13, 2009.

Aviation Security: Transportation Security Administration Has Strengthened Planning to Guide Investments in Key Aviation Security Programs, but More Work Remains. GAO-08-1024T. Washington, D.C.: July 24, 2008.

Transportation Security: TSA Has Developed a Risk-Based Covert Testing Program, but Could Better Mitigate Aviation Security Vulnerabilities Identified Through Covert Tests. GAO-08-958. Washington, D.C.: August 8, 2008.

Mass Transit and Passenger Rail Security

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

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.

Highway Infrastructure Security

Commercial Vehicle Security: Risk-Based Approach Needed to Secure the Commercial Vehicle Sector. GAO-09-85. Washington, D.C.: February 27, 2009.

Highway Infrastructure: Federal Efforts to Strengthen Security Should Be Better Coordinated and Targeted on the Nation's Most Critical Highway Infrastructure. GAO-09-57. Washington, D.C.: January 30, 2009.

Cross-Cutting Issues

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 Worker Identification Credential: Progress Made in Enrolling Workers and Activating Credentials but Evaluation Plan Needed to Help Inform the Implementation of Card Readers. GAO-10-43. Washington, D.C.: November 18, 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.

Transportation Security: Efforts to Strengthen Aviation and Surface Transportation Security Continue to Progress, but More Work Remains. GAO-08-651T. Washington, D.C.: April 15, 2008.

GAO Contact and Staff Acknowledgements

GAO Contact

Charles Jeszeck, (202) 512-8777 or jeszeckc@gao.gov.

Acknowledgments

In addition to the contact name above, Jessica Lucas-Judy, Assistant Director, and Jonathan R. Tumin, analyst-in-charge, managed this assignment. Anthony Fernandez contributed to all aspects of the work. Debra Sebastian, Chris Currie, Adam Vogt, and Katherine Davis assisted in report development.

(440826)

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