

GAO

Report to the Chairman, Committee on
Homeland Security, House of
Representatives

June 2009

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

Accountability * Integrity * Reliability



Highlights of [GAO-09-678](#), a report to the Chairman, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

Terrorist incidents worldwide have highlighted the need for securing mass transit and passenger rail systems. The Department of Homeland Security's (DHS) Transportation Security Administration (TSA) is the primary federal entity responsible for securing these systems. GAO was asked to assess (1) the extent to which federal and industry stakeholders have assessed risks to these systems since 2004, and how TSA has used this information to inform its security strategy; (2) key actions federal and industry stakeholders have taken since 2004 and the extent to which federal actions are consistent with TSA's security strategy, and the challenges TSA faces in implementing them; and (3) TSA's reported status in implementing 9/11 Commission Act provisions for mass transit and passenger rail security. GAO reviewed documents including TSA's mass transit and passenger rail strategic plan, and interviewed federal officials and industry stakeholders from 30 systems and Amtrak—representing 75 percent of U.S. mass transit and passenger rail ridership.

What GAO Recommends

Among other things, GAO recommends that TSA conduct a risk assessment that includes all elements of risk, enhance its security strategy by incorporating performance measures, improve sharing of security technology information, and develop a plan with milestones for meeting 9/11 Act provisions. DHS concurred with GAO's recommendations.

View [GAO-09-678](#) or [key components](#). For more information, contact Cathy Berrick at (202) 512-3404 or berrickc@gao.gov.

TRANSPORTATION SECURITY

Key Actions Have Been Taken to Enhance Mass Transit and Passenger Rail Security, but Opportunities Exist to Strengthen Federal Strategy and Programs

What GAO Found

Since 2004, federal and industry stakeholders have conducted assessments of individual elements of risk—threat, vulnerability and consequence—for mass transit and passenger rail systems and this information has informed TSA's security strategy; however, TSA has not combined information from these three elements to conduct a risk assessment of these transportation systems. By completing a risk assessment, TSA would have reasonable assurance that it is directing its resources toward the highest priority needs. Further, while TSA's mass transit and passenger rail security strategy contains some information, such as goals and objectives, that is consistent with GAO's prior work on characteristics of a successful national strategy, it could be strengthened by including performance measures to help TSA track progress in securing these systems, among other things.

Federal and industry stakeholders have taken several key actions to strengthen the security of mass transit and passenger rail systems since 2004, and while federal actions have been generally consistent with TSA's security strategy, TSA faces coordination challenges, and opportunities exist to strengthen some programs. TSA has deployed surface inspectors to assess industry security programs and worked with DHS to develop security technologies, among other actions. Mass transit and passenger rail systems, including Amtrak, also reported taking actions to increase security, such as implementing passenger and baggage screening programs. Although TSA has taken steps to enhance its efforts, it can further strengthen security programs by, for example, expanding its efforts to obtain and share security technology information with industry. By improving information sharing with industry, TSA can help to ensure that its and industry's limited resources are used more productively to secure mass transit and passenger rail systems.

As of March 2009, TSA reported implementing some of the 9/11 Commission Act provisions related to securing mass transit and passenger rail such as developing a strategy for securing transportation, but had missed deadlines, for example, for issuing new regulatory requirements for mass-transit and passenger-rail employee security training. In addition, TSA's progress reports that track its implementation of 9/11 Act provisions lack milestones to guide this effort as called for by project management best practices. Additionally, in some cases, TSA progress reports identify challenges to meeting 9/11 Act provisions, but these reports do not include a plan for addressing these challenges. Until TSA develops a plan with milestones, it will be difficult for TSA to provide reasonable assurance that the act's provisions are being implemented and that a plan is in place for overcoming challenges that arise. Additionally, officials from almost half of the mass transit and passenger rail systems GAO visited reported concerns with the potential costs and the feasibility of implementing pending employee security training requirements.

Contents

Letter		1
	Background	6
	Federal and Industry Stakeholders Have Assessed Individual Elements of Risk, Which Have Informed TSA's Security Strategy, but TSA Could Strengthen Its Approach by Conducting a Risk Assessment and Updating Its Security Strategy	15
	Federal and Industry Stakeholders Have Taken Key Actions to Strengthen Transit Security and Federal Actions Have Been Generally Consistent with TSA's Strategy, but Opportunities Exist to Strengthen Some Programs	33
	TSA Reported Implementing Some 9/11 Commission Act Provisions for Mass Transit and Passenger Rail Security, but Implementing New Regulations May Pose Challenges for TSA and Industry Stakeholders	50
	Conclusions	58
	Recommendations for Executive Action	60
	Agency Comments	61
Appendix I	Objectives, Scope, and Methodology	65
Appendix II	TSA/FTA Security and Emergency Management Action Items	72
Appendix III	Identifying Characteristics of Successful National Strategies in the Context of Mass Transit and Passenger Rail Security	74
Appendix IV	Federal Actions Taken to Enhance Mass Transit and Passenger Rail Security since 2004	78
Appendix V	Modal Annex Objectives and Examples of Actions Taken to Achieve Them as of February 2009	82

Appendix VI	DHS Mass Transit and Passenger Rail Related Security Technology Pilots Conducted from 2004 to 2009	83
Appendix VII	Comments from Amtrak	86
Appendix VIII	Comments from the Department of Homeland Security	88
Appendix IX	GAO Contacts and Staff Acknowledgments	93

Tables

Table 1: Summary of Federal and Industry Stakeholders' Assessment Activities since 2004	16
Table 2: Summary of Federal and Industry Stakeholders' Assistance to Transit Agencies for Risk Assessments Provided since 2004	18
Table 3: Summary of Desirable Characteristics of Successful National Strategies and Related Executive Order Factors	27
Table 4: Sector Goals and Passenger Rail and Mass Transit Subordinate Objectives to Complete Sector Goals	30
Table 5: Key Federal Actions Taken to Enhance Mass Transit and Passenger Rail Security Since 2004	35
Table 6: Key Selected Provisions of the 9/11 Commission Act for Mass Transit and Passenger Rail Security and TSA's Reported Implementation Status, as of March 2009	51
Table 7: Mass Transit and Passenger Rail Systems Interviewed	68
Table 8: Federal Actions Taken to Enhance Mass Transit and Passenger Rail Security since 2004	78
Table 9: TSA Mass Transit Modal Annex Objectives and Examples of Actions That Have Been Employed to Achieve the Objectives, as of February 2009	82
Table 10: DHS Mass Transit and Passenger Rail Related Security Technology Pilots Conducted from 2004 to 2009	83

Figures

Figure 1: Geographic Distribution of Amtrak and Rail Transit Systems in the United States	7
Figure 2: NIPP Risk Management Framework	14
Figure 3: Photo of DHS S&T Pilot Technology for a Fare Card Vending Machine with Explosive Trace Detection Capability	41

Abbreviations

AAR	after-action report
APTA	American Public Transportation Association
ASFD-S	Assistant Federal Security Director-Surface
BASE	Baseline Assessment for Security Enhancement
CI/KR	critical infrastructure and key resource
CONOPS	Concept of Operations
DHS	Department of Homeland Security
DHS S&T	Department of Homeland Security Science and Technology Directorate
DOT	Department of Transportation
FEMA	Federal Emergency Management Administration
FRA	Federal Railroad Administration
FTA	Federal Transit Administration
GCC	Government Coordinating Council
HITRAC	Homeland Infrastructure Threat Reporting and Analysis Center
HSIN	Homeland Security Information Network
HSPD-7	Homeland Security Presidential Directive 7
IED	improvised explosive device
IPT	Integrated Product Team
MOU	memorandum of understanding
NPPD	National Protection and Programs Directorate
NSTS	National Strategy for Transportation Security
NTI	National Transit Institute
ODP	Office of Domestic Preparedness
PAG	Transit Policing and Security Peer Advisory Group
PART	Program Assessment Rating Tool
SAAP	Security Analysis and Action Program
SCC	Sector Coordinating Council
SEMTAP	Security and Emergency Management Technical Assistance Program

SHIRA	Strategic Homeland Infrastructure Risk Assessment
SSA	sector-specific agency
STSIP	Surface Transportation Security Inspection Program
TRAM	Transit Risk Assessment Methodology
TSA	Transportation Security Administration
TSA-OI	TSA Office of Intelligence
TSGP	Transit Security Grant Program
TSI-S	Transportation Security Inspector-Surface
TSNM	Transportation Sector Network Management
TS-SSP	Transportation Systems-Sector Specific Plan
VIPR	Visible Intermodal Prevention and Response

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office
Washington, DC 20548

June 24, 2009

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
House of Representatives

Dear Mr. Chairman:

Mass transit and passenger rail systems are vital components of the nation's transportation infrastructure, encompassing rail transit (heavy rail, commuter rail, and light rail), intercity rail, and transit bus systems.¹ In the United States, mass transit and passenger rail systems provide approximately 34 million passenger trips each weekday, and commuters rely on these systems to provide efficient, reliable and safe transportation.² However, terrorist attacks on mass transit and passenger rail systems around the world—such as the 2006 passenger train bombing in Mumbai, India that resulted in 209 fatalities—highlight the vulnerability of these systems and the need for an increased focus on securing them from terrorism. While there have been no terrorist attacks against U.S. mass transit and passenger rail systems to date, 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, an

¹ Mass transit and passenger rail systems consist of various bus and passenger rail transit systems. Transit bus includes inter-city bus or trolleybus systems. Transit rail is comprised of heavy, commuter, light and intercity rail systems. Heavy rail is an electric railway that can carry a heavy volume of traffic. Heavy rail is characterized by high speed and rapid acceleration, passenger rail cars operating singly or in multi-car trains on fixed rails, separate rights of way from which all other vehicular and foot traffic is excluded, sophisticated signaling, and high-platform loading. Most subway systems are considered heavy rail. Commuter rail is characterized by passenger trains operating on railroad tracks and providing regional service, such as between a central city and its adjacent suburbs. Light rail systems typically operate passenger rail cars singly (or in short, usually two-car, trains) and are driven electrically with power being drawn from an overhead electric line. Amtrak operates the nation's primary intercity rail system.

² The American Public Transportation Association compiled this ridership data from the Federal Transit Administration's National Transit Database. Ridership on rail transit systems in the District of Columbia and Puerto Rico are included in these statistics. A passenger trip is defined as the number of passengers who board public transportation vehicles. Passengers are counted each time they board vehicles no matter how many vehicles they use to travel from their origin to their destination.

attack on these systems could potentially lead to significant casualties due to the high number of daily transit passengers, especially during peak commuting hours.

While several entities play a role in helping to fund and secure U.S. mass transit and passenger rail systems, the Department of Homeland Security's (DHS) Transportation Security Administration (TSA) is the primary federal agency responsible for overseeing security for these systems and for developing a national strategy and implementing programs to enhance their security. Additionally, several DHS components—with assistance from the Department of Transportation's (DOT) Federal Transit Administration (FTA) and Federal Railroad Administration (FRA)—are to conduct threat and vulnerability assessments of mass transit and passenger rail systems, research and develop security technologies for these systems, and develop security training programs for mass transit and passenger rail employees. Day-to-day responsibility for securing mass transit and passenger rail systems falls on mass transit and passenger rail agencies themselves, local law enforcement, and often state and local governments that own a significant portion of the infrastructure. The partnership of federal and non-federal mass transit and passenger rail stakeholders was strengthened following the terrorist attacks of September 11th, in part, by collaborating to implement a variety of security programs. In addition, the passage of the Implementing Recommendations of the 9/11 Commission Act (9/11 Commission Act) in August 2007 requires DHS to further expand its roles and responsibilities for securing mass transit and passenger rail in several areas, such as by conducting and updating security assessments and issuing new regulations that will establish new security requirements for mass transit and passenger rail agencies to implement.³

You requested that we evaluate TSA's mass transit and passenger rail security strategy and supporting programs and activities, as well as TSA's efforts to assess the impact of these initiatives on U.S. mass transit and passenger rail systems since TSA's issuance of passenger rail security

³ Pub. L. No. 110-53, 121 Stat. 266 (2007).

directives in 2004.⁴ Specifically, this report addresses the following questions:

- To what extent have federal and industry stakeholders assessed or supported assessments of the security risks to mass transit and passenger rail since 2004, and how, if at all, has TSA used risk assessment information to inform and update its security strategy?
- What key actions, if any, have federal and industry stakeholders implemented or initiated, since 2004, to strengthen the security of mass transit and passenger rail systems; to what extent are federal actions consistent with TSA's security strategy; and what challenges, if any, does TSA face in implementing them?
- What is TSA's reported status in implementing provisions of the Implementing Recommendations of the 9/11 Commission Act of 2007 related to mass transit and passenger rail security, and what challenges, if any, does TSA and mass transit and passenger rail industry face in implementing the actions required by the act?

To determine the extent to which federal and industry stakeholders assessed security risks to mass transit and passenger rail systems since 2004, we analyzed various assessment reports from DHS component agencies, including TSA, DHS's Office of Infrastructure Protection within the National Protection and Programs Directorate (NPPD), and the Homeland Infrastructure Threat Reporting and Analysis Center (HITRAC), as well as FTA and stakeholders outside of the federal government.⁵ Because of the scope of our work, we relied on TSA to identify its assessment activities but did not assess the extent to which its assessment activities meet the National Infrastructure Protection Plan (NIPP) criteria for threat, vulnerability, and consequence assessments. In addition, we analyzed TSA's security strategy for the mass transit and passenger rail systems—the Mass Transit Modal Annex—to determine the extent to which it addressed the threats, vulnerabilities, and consequences

⁴ According to TSA's fiscal year 2009 Surface Transportation Security Inspection Program Annual Domestic Inspection and Assessment Plan, a security directive is a mandatory measure or measures issued by TSA in response to a threat assessment or to a specific threat against transportation, requiring affected transportation organizations to implement specified security measures. TSA issued two security directives in May 2004 after terrorists attacked the commuter rail system in Madrid, Spain. The directives mandated passenger rail systems and Amtrak to implement a number of security measures.

⁵ For the purpose of this report, industry stakeholders include mass transit and passenger rail systems, Amtrak and an industry association.

identified in the assessments we reviewed. We also analyzed requirements pertaining to mass transit and passenger rail security assessments and strategy including Executive Order 13416: *Strengthening Surface Transportation Security*, to determine the extent to which TSA's security strategy conformed to requirements.⁶ We analyzed executive guidance including the NIPP and the Transportation Systems-Sector Specific Plan (TS-SSP) to determine the best practices for effectively implementing a risk management framework and associated best practices for conducting risk assessments. We also reviewed guidance on strategic planning that GAO developed in a previous report.⁷

To determine key actions federal and industry stakeholders have initiated or implemented since 2004 to strengthen mass transit and passenger rail security, we analyzed documentation on DHS and DOT mass transit and passenger rail security programs, including the Mass Transit Modal Annex, after action reports of TSA security operations, and security technology information on DHS's Homeland Security Information Network (HSIN) Public Transit Portal. We also interviewed federal stakeholders, including DHS representatives from TSA, the DHS Science and Technology Directorate (DHS S&T), and HITRAC, and DOT representatives from FTA and FRA.⁸ Additionally, we analyzed federal actions against the objectives outlined in TSA's security strategy—the Mass Transit Modal Annex—to determine whether these actions were consistent with the strategy. To identify implementation challenges with these actions, we interviewed federal and transit agency stakeholders involved in either developing or participating in these programs. We conducted site visits, or held teleconferences with, security and management officials from 30 mass transit and passenger rail agencies across the nation. Additionally, we met with officials from two regional transit authorities and Amtrak officials responsible for overall systems security as well as individual station security personnel. The entities we interviewed represent 75 percent of the nation's total mass transit and passenger rail ridership based on

⁶ Exec. Order No. 13416, 71 Fed. Reg. 71033 (Dec. 5, 2006).

⁷ GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, [GAO-04-408T](#) (Washington, D.C.: Feb. 3, 2004).

⁸ DHS S&T was established by the Homeland Security Act of 2002 to, among other things, coordinate the federal government's civilian efforts to identify and develop countermeasures to emerging terrorist threats to the United States. As DHS's primary research and development arm, DHS S&T is tasked with providing federal, state, local, and tribal officials with state of the art technology and other resources.

information we obtained from the Federal Transit Administration's National Transit Database and the American Public Transportation Association. Because we selected a non-probability sample of mass transit and passenger rail agencies, the results from these visits and teleconferences cannot be generalized to all mass transit and passenger rail agencies; however, information we obtained provided us with an broad overview of the types of key actions taken to strengthen security.

To determine TSA's reported status in implementing mass transit and passenger rail provisions of the 9/11 Commission Act and challenges TSA and industry stakeholders may face in implementing actions required by the act, we analyzed TSA documentation outlining the agency's status in fulfilling various requirements and documentation on TSA's Surface Transportation Security Inspection Program. We also interviewed officials from TSA's Surface Transportation Security Inspection Program, including headquarters officials, and inspectors from 13 of 54 field office locations, including 11 of 12 Assistant Federal Security Directors for Surface (supervisors for primary field offices) regarding how the 9/11 Commission Act requirements may affect their job responsibilities. We interviewed officials from all inspection program field locations that have oversight responsibility for the mass transit and passenger rail agencies we interviewed. Because we selected a non-probability sample of TSA's Surface Transportation Security Inspection Program field offices, the results from these interviews cannot be generalized to all Surface Transportation Security Inspection Program field offices; however, information we obtained provided us with an overview of the potential impact of the 9/11 Commission Act on field operations.

We conducted this performance audit from September 2007 through June 2009 in accordance with generally accepted government auditing standards. Those 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 and conclusions based on our audit objectives.

Background

Overview of U.S. Mass Transit and Passenger Rail Systems

Mass transit and passenger rail systems provided 10.7 billion passenger trips in the United States in fiscal year 2008.⁹ The nation's mass transit and passenger rail systems include all multiple-occupancy vehicle services designed to transport customers on local and regional routes, such as transit buses, heavy rail, commuter rail, and light rail services, and the interconnected facilities and vehicles feeding into the transit systems. Buses are the most widely used form of transit, providing almost two-thirds of all passenger trips. Heavy rail systems—subway systems like New York City's transit system and Washington, D.C.'s Metro—typically operate on fixed rail lines within a metropolitan area and have the capacity for a heavy volume of traffic. Commuter rail systems typically operate on railroad tracks and provide regional service (e.g., between a central city and adjacent suburbs). Light rail systems are typically characterized by lightweight passenger rail cars that operate on track that is not separated from vehicular traffic for much of the way. Mass transit and passenger rail systems in the United States are typically owned and operated by public sector entities, such as state and regional transportation authorities.

Amtrak, which reported that it provided 25.8 million passenger trips in fiscal year 2007, operates the nation's primary intercity passenger rail and serves more than 500 stations in 46 states and the District of Columbia.¹⁰ Amtrak operates over a 22,000 mile network, primarily over leased freight railroad tracks. In addition to leased tracks, Amtrak owns about 650 miles of track, primarily on the "Northeast Corridor" between Boston and Washington, D.C., which carries about two-thirds of Amtrak's total ridership. Stations are owned by Amtrak, freight carriers, municipalities, and some private entities. Amtrak also operates commuter rail services in certain jurisdictions on behalf of state and regional transportation authorities. Figure 1 identifies the geographic distribution of rail transit systems and Amtrak within the United States. Though not indicated on the map, all of these cities also have bus transit systems.

⁹ Ridership data reported by the American Public Transportation Association for 2008.

¹⁰ The Alaska Railroad Corporation also operates intercity passenger rail service. Amtrak's ridership data comes from the 2007 Amtrak Environmental Health and Safety Report, which is the most recently available data.

Figure 1: Geographic Distribution of Amtrak and Rail Transit Systems in the United States



Source: Amtrak and National Transit Database; Map Resources (map).

Mass Transit and Passenger Rail Systems Are Inherently Vulnerable to Terrorist Attacks

To date, U.S. mass transit and passenger rail systems have not been attacked by terrorists. However, these systems have received heightened attention as several alleged terrorists' plots have been uncovered, including multiple plots involving systems in the New York City area. Worldwide, mass transit and passenger rail systems have been the

frequent target of terrorist attacks. According to the Worldwide Incidents Tracking System maintained by the National Counter-Terrorism Center, from January 2004 to July 2008, there were 530 terrorist attacks worldwide against mass transit and passenger rail targets, resulting in over 2,000 deaths and over 9,000 injuries. Terrorist attacks include a 2007 attack on a passenger train in India (68 fatalities and over 13 injuries); the 2005 attack on London's underground rail and bus systems (52 fatalities and over 700 injuries); and the 2004 attack on commuter rail trains in Madrid (191 fatalities and over 1,800 injuries). In January 2008, Spanish authorities arrested 14 suspected terrorists who were allegedly connected to a plot to conduct terrorist attacks in Spain, Portugal, Germany, and the United Kingdom, including an attack on the Barcelona metro subway system. The most common means of attack against mass transit and passenger rail systems has been improvised explosive devices (IED), with many of these attacks delivered by suicide bombers.¹¹

According to transit agency officials, certain characteristics of mass transit and passenger rail systems make them inherently vulnerable to terrorist attacks and therefore difficult to secure. By design, mass transit and passenger rail systems are open (i.e., have multiple access points, hubs serving multiple carriers, and, in some cases, no barriers to access) so that they can move large numbers of people quickly. The openness of these systems can leave them vulnerable because operator personnel cannot completely monitor or control who enters or leaves the systems. In addition, other characteristics of mass transit and passenger rail systems—high ridership, expensive infrastructure (more so for passenger rail than bus), economic importance, and location in large metropolitan areas or tourist destinations—also make them attractive targets for terrorists because of the potential for mass casualties, economic damage and disruption. Moreover, some of these same characteristics make them difficult to secure. For example, the number of riders passing through a subway system—especially during peak hours—may make the sustained use of some security measures, such as airport style passenger screening checkpoints, difficult because the measures could disrupt scheduled service. In addition, multiple access points along extended routes may make securing each location difficult because of the costs associated with

¹¹ An IED, or “homemade bomb,” is typically constructed of commonly available materials, and can be carried by an individual or deposited in an unnoticed location for detonation by a timer or remote control.

such actions. Balancing the potential economic impacts of security enhancements with the benefits of such measures is a difficult challenge.

Multiple Stakeholders Share Responsibility for Securing Mass Transit and Passenger Rail Systems

Securing the nation's mass transit and passenger rail systems is a shared responsibility requiring coordinated action on the part of federal, state, and local governments; the private sector; and passengers who ride these systems. Since the September 11, 2001 attacks, the role of federal agencies in securing the nation's transportation systems has continued to evolve. In response to the September 11th terrorist attacks, Congress passed the Aviation and Transportation Security Act of 2001, which created TSA within DOT and conferred to the agency broad responsibility for overseeing the security of all modes of transportation, including mass transit and passenger rail.¹² In 2002, Congress passed the Homeland Security Act, which established DHS, transferred TSA from DOT to DHS, and assigned DHS responsibility for protecting the nation from terrorism, including securing the nation's transportation systems.¹³ Within TSA, the office of Transportation Sector Network Management (TSNM) leads the unified effort to protect and secure the nation's intermodal transportation systems, with divisions dedicated to each transportation mode, including mass transit and passenger rail. Within TSA's Office of Security Operations, the Office of Multi-modal Oversight manages the Surface Transportation Security Inspection Program which coordinates with TSNM to develop and implement security programs, including strategies for conducting and implementing assessments and other actions in mass transit and passenger rail. In addition, TSA's Office of Intelligence (TSA-OI) is responsible for collecting and analyzing threat information related to the transportation network, which includes all modes of transportation. TSA is supported in these efforts by other DHS entities such as the NPPD and the Federal Emergency Management Agency's (FEMA) Grant Programs Directorate and Planning and Assistance Branch. The NPPD is responsible for coordinating efforts to protect the nation's most critical assets across all 18 industry sectors, including surface transportation.¹⁴

¹² Pub. L. No. 107-71, 115 Stat. 597 (2001). A mode of transportation refers to the different means that are used to transport people or cargo.

¹³ Pub. L. No. 107-296, 116 Stat. 2135 (2002).

¹⁴ 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.

FEMA's Grant Programs Directorate is responsible for managing DHS grants for mass transit. FEMA's Planning and Assistance Branch is responsible for assisting transit agencies with how to conduct risk assessments.

TSA has issued requirements related to the security of mass transit and passenger rail systems. Specifically, in May 2004, TSA issued security directives that mandated passenger rail agencies and Amtrak to implement certain security measures, such as periodically inspecting passenger rail cars for suspicious or unattended items and reporting potential threats or significant security concerns to appropriate law enforcement authorities and TSA.¹⁵ In addition to these requirements, in August 2007, the 9/11 Commission Act was signed into law, which included provisions that task TSA with security actions related to mass transit and passenger rail security. Among other things, these provisions include mandates for developing and issuing reports on TSA's strategy for securing public transportation, conducting and updating security assessments of mass transit systems, and establishing a program for conducting security exercises for transit and rail agencies.

While TSA is the lead federal agency for overseeing the security of all transportation modes, DOT continues to play a key supporting role in securing mass transit and passenger rail systems. In a 2004 memorandum of understanding (MOU) and a 2005 annex to the MOU, TSA and FTA agreed that the two agencies would coordinate their programs and services, with FTA playing a supporting role by providing technical assistance and assisting DHS with implementation of its security policies, including collaborating in developing regulations affecting transportation security. In particular, FTA has played a role in coordinating and funding security training programs for mass transit and passenger rail employees, and provided dedicated funding to three federal training providers to implement mass transit and passenger rail employee training programs. Additionally, FTA administers the State Safety Oversight program and may withhold federal funding for states' noncompliance with regulations

¹⁵ On November 26, 2008, TSA published a final rule that included some of the provisions in the security directives, including requirements for passenger rail systems to appoint a security coordinator and report potential threats and significant security concerns to TSA. 73 Fed. Reg. 72130 (Nov. 26, 2008).

governing state safety oversight agencies.¹⁶ As part of this program, state safety oversight agencies are responsible for reviewing and approving rail transit agencies' safety and security plans, among other activities. FTA also promotes mass transit and passenger rail safety and security by providing funding for research, technical assistance, and technology demonstration projects. In addition to FTA, DOT's FRA also has regulatory authority over commuter rail operators and Amtrak and employs over 400 inspectors who periodically monitor the implementation of safety and security plans at these systems. FRA regulations require railroads that operate intercity or commuter passenger train service or that host the operation of that service to adopt and comply with a written emergency preparedness plan approved by FRA.¹⁷

State and local governments, mass transit and passenger rail operators, and private industry are also important stakeholders in the nation's mass transit and passenger rail security efforts. State and local governments, in some cases, own or operate a significant portion of mass transit and passenger rail systems. Consequently, the responsibility for responding to emergencies involving systems that run through their jurisdictions often falls to state and local governments. Although all levels of government are involved in mass transit and passenger rail security, the primary responsibility for securing the systems rests with the mass transit and passenger rail operators. These operators, which can be public or private entities, are responsible for administering and managing transit activities and services, including security. They can also directly operate the security service provided or contract for all or part of the total service. We discuss security actions taken by federal agencies and mass transit and passenger rail system operators later in this report.

¹⁶ Through 49 C.F.R. pt. 659, FTA requires states to designate an agency to conduct tri-annual safety and security audits of the nation's light or heavy rail systems. These agencies are called state safety oversight agencies.

¹⁷ According to FRA, the regulation makes clear that an "emergency" includes a security-related situation. Each plan must address employee training and qualification, and provide for training and coordination with emergency responders. Also, each covered railroad must conduct full-scale passenger train emergency simulations in order to determine its capability to execute the emergency preparedness plan.

A Risk-Based Approach to Mass Transit and Passenger Rail Security

In recent years, we, along with the Congress, the executive branch, and the 9/11 Commission have recommended that federal agencies with homeland security responsibilities utilize a risk management approach to help ensure that finite national resources are dedicated to assets or activities considered to have the highest security priority.¹⁸ We have concluded that without a risk management approach, there is limited assurance that programs designed to combat terrorism would be properly prioritized and focused.¹⁹ Thus, risk management, as applied in the homeland security context, can help to more effectively and efficiently prepare defenses against acts of terrorism and other threats.

Homeland Security Presidential Directive 7 (HSPD-7) directed the Secretary of Homeland Security to establish uniform policies, approaches, guidelines, and methodologies for integrating federal infrastructure protection and risk management activities. Recognizing that each sector possesses its own unique characteristics and risk landscape, HSPD-7 designates federal government sector specific agencies (SSA) for each of the critical infrastructure sectors that are to work with DHS to improve critical infrastructure security.²⁰ On June 30, 2006, DHS released the National Infrastructure Protection Plan (NIPP), which created—in accordance with HSPD-7—a risk-based framework for the development of SSA strategic plans.²¹ As the SSA for transportation, TSA developed the

¹⁸ The 9/11 Commission was one of the congressionally chartered commissions established by Congress on November 27, 2002 to (1) investigate the relevant facts and circumstances relating to the terrorist attacks of September 11, 2001; (2) identify, review, and evaluate lessons learned from these attacks; and (3) report to the President and the Congress on findings, conclusions, and recommendations that generated from the investigation and review.

¹⁹ GAO, *Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts*, [GAO-05-851](#) (Washington, D.C.: September 2005).

²⁰ Sector-specific agencies (SSA) refer to the federal department or agency responsible for infrastructure protection activities in a designated critical infrastructure sector or key resources category.

²¹ DHS serves as the sector-specific agency for 11 of the 18 sectors: information technology; communications; transportation systems; chemical; emergency services; nuclear reactors, material, and waste; postal and shipping; dams; government facilities; and commercial facilities; and critical manufacturing. Other sector-specific agencies such as the departments of Agriculture, Defense, Energy, Health and Human Services, the Interior, the Treasury, and the Environmental Protection Agency are responsible for the other 7 sectors: agriculture and food; defense industrial base; energy; healthcare and public health; national monuments and icons; banking and finance; and water. See GAO, *Critical Infrastructure Protection: Sector Plans and Sector Councils Continue to Improve*, [GAO-07-706R](#) (Washington D.C.: July 10, 2007).

Transportation Systems—Sector Specific Plan (TS-SSP) in 2007 to document the process to be used in carrying out the national strategic priorities outlined in the NIPP and the National Strategy for Transportation Security (NSTS).²² The TS-SSP contains supporting modal implementation plans for each transportation mode, including mass transit and passenger rail, which provides information on current efforts to secure mass transit and passenger rail, as well as TSA’s overall goals and objectives related to mass transit and passenger rail security.²³

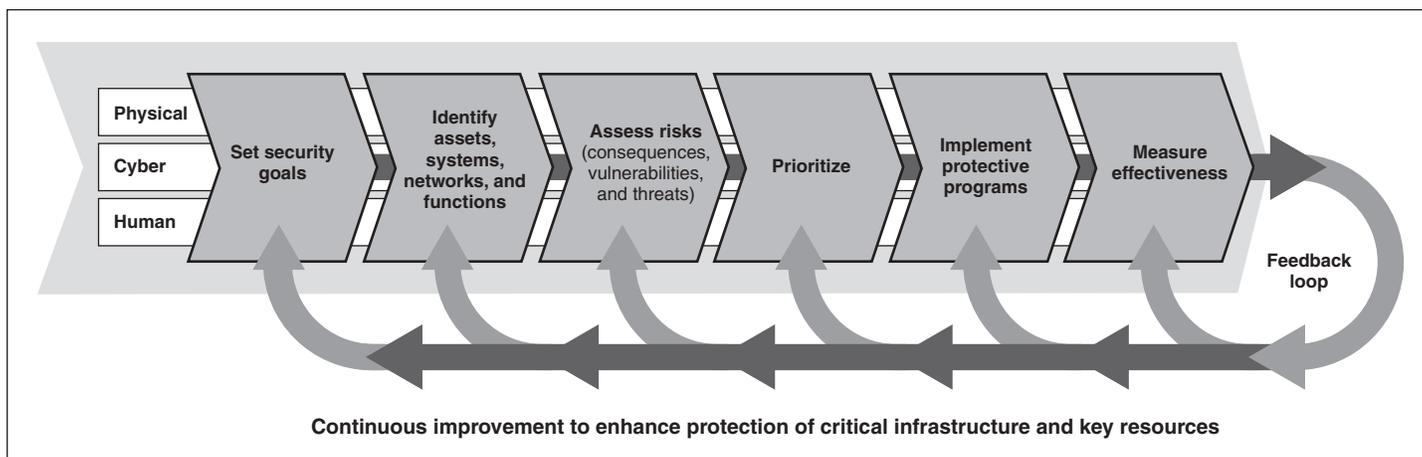
The NIPP defines roles and responsibilities for security partners in carrying out critical infrastructure and key resource (CI/KR) protection activities through the application of risk management principles.²⁴ Figure 2 illustrates the several interrelated activities of the risk management framework as defined by the NIPP. The NIPP requires that federal agencies use this information to inform the selection of risk-based priorities and the continuous improvement of security strategies and programs to protect people and critical infrastructure by reducing the risk of acts of terrorism.

²² The NSTS, mandated in the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), outlines the federal government approach—in partnership with state, local, and tribal governments and private industry—to secure the U.S. transportation system from terrorist threats and attacks.

²³ DHS updated its NIPP in 2009.

²⁴ Critical infrastructure are systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters. Key resources are publicly or privately controlled resources essential to minimal operations of the economy or government, including individual targets whose destruction would not endanger vital systems but could create a local disaster or profoundly damage the nation’s morale or confidence.

Figure 2: NIPP Risk Management Framework



Source: DHS.

Within the risk management framework, the NIPP also establishes baseline criteria for conducting risk assessments. According to the NIPP, risk assessments are a qualitative and/or quantitative determination of the likelihood of an adverse event occurring and are a critical element of the NIPP risk management framework. Risk assessments can also help decision makers identify and evaluate potential risks so that countermeasures can be designed and implemented to prevent or mitigate the potential effects of the risks.

The NIPP characterizes risk assessment as a function of three elements:

- **Threat:** The likelihood that a particular asset, system, or network will suffer an attack or an incident. In the context of risk associated with a terrorist attack, the estimate of threat is based on the analysis of the intent and the capability of an adversary; in the context of a natural disaster or accident, the likelihood is based on the probability of occurrence.
- **Vulnerability:** The likelihood that a characteristic of, or flaw in, an asset, system, or network's design, location, security posture, process, or operation renders it susceptible to destruction, incapacitation, or exploitation by terrorist or other intentional acts, mechanical failures, and natural hazards.
- **Consequence:** The negative effects on public health and safety, the economy, public confidence in institutions, and the functioning of government, both direct and indirect, that can be expected if an asset,

system, or network is damaged, destroyed, or disrupted by a terrorist attack, natural disaster, or other incident.

Information from the three elements that assess risk—threat, vulnerability and consequence—can lead to a risk characterization and provide input for prioritizing security goals.

Federal and Industry Stakeholders Have Assessed Individual Elements of Risk, Which Have Informed TSA’s Security Strategy, but TSA Could Strengthen Its Approach by Conducting a Risk Assessment and Updating Its Security Strategy

Since 2004, federal and industry stakeholders have conducted assessments of individual elements of risk—threat, vulnerability and consequence—and this information has informed TSA’s mass transit and passenger rail security strategy. However, TSA could strengthen its approach by using and combining this information to conduct a risk assessment of the mass transit and passenger rail system and by updating its strategy to include characteristics that we identified as desirable practices for successful national strategies and to more fully address elements that are outlined in Executive Order 13416: *Strengthening Surface Transportation Security*.²⁵

Federal and Industry Stakeholders Have Conducted Assessments of Individual Elements of Risk, but TSA Could Strengthen Its Approach by Conducting a Risk Assessment

While federal and industry stakeholders have conducted assessments of individual elements of risk—threat, vulnerability, and consequence—TSA could strengthen its security approach by using and combining this information to conduct a risk assessment of the mass transit and passenger rail system. 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. Since 2004, federal agencies have conducted a range of assessment activities related to the individual elements of risk to help determine their strategy for securing mass transit and passenger rail systems, and provided guidance to mass transit and

²⁵ [GAO-04-408T](#) and Exec. Order No. 13416, 71 Fed. Reg. 71033 (Dec. 5, 2006).

passenger rail agencies on how to conduct assessments of individual elements of risk. For example, DHS's threat assessments considered potential threats to the mass transit and passenger rail system, while vulnerability assessments focused on mass transit and passenger rail systems' security conditions or specific infrastructure such as tunnels. In addition to DHS assessments, DOT provided assistance to mass transit and passenger rail agencies on how to conduct threat and vulnerability assessments, and transit agencies have reported conducting risk assessments for their own systems or assets. See table 1 for a summary of federal and industry stakeholders' assessment activities related to individual elements of risk.

Table 1: Summary of Federal and Industry Stakeholders' Assessment Activities since 2004

Entity	Time frame	Description	Risk Elements		
			T	V	C
DHS Transportation Security Administration (TSA)					
Office of Intelligence	2008	Annual Threat Assessments: TSA's Office of Intelligence provides an overview of threats—including key actors and possible attack tactics and targets—to mass transit and passenger rail systems. The assessment includes incidents of interest and suspicious activities targeting mass transit and passenger rail in the United States and overseas.	•		
Transportation Sector Network Management (TSNM)/ Surface Transportation Security Inspection Program (STSIP)	2006-present	Baseline Assessment for Security Enhancement (BASE): Surface inspectors, in coordination with transit agency officials, assess a transit agency's overall security posture, focusing on the implementation and effectiveness of security plans, programs and measures, security gaps, and best practices. Since 2006, TSA reported it has conducted BASE reviews at 91 of the top 100 largest mass transit and passenger rail agencies in the nation and has initiated follow-on BASE reviews to determine if previously identified security shortfalls have been corrected.		•	
DHS National Protection and Programs Directorate (NPPD)					
Homeland Security Threat and Risk Analysis Center (HITRAC)	2008	Strategic Homeland Infrastructure Risk Assessment (SHIRA): Annual document assessing risk across each of the 18 CI/KR sectors including mass transit and passenger rail. Includes threat scenarios identified by HITRAC and vulnerability and consequence information provided by each CI/KR sector.	•	(•) ^a	(•) ^a

Entity	Time frame	Description	Risk Elements		
			T	V	C
DHS Science and Technology Directorate (DHS S&T)					
Science and Technology Directorate (DHS S&T)	2007	Transit Tunnel Vulnerability Assessments: DHS S&T, in coordination with TSNM-Mass Transit and National Laboratories, assessed the vulnerabilities of transit tunnels and potential consequences to tunnel structures resulting from various types of explosive threats. S&T also assists transit agencies with planning and implementing protective measures to deter and prevent terrorist attacks.		•	•
Industry Stakeholders					
National Railroad Passenger Corporation (Amtrak)	2007-present	Risk Assessment: Amtrak has reported conducting risk assessments that incorporate and combine all three elements of risk (threat, vulnerability, and consequence) for all of its systems.	•	•	•
Transit Systems	2008-present	Risk Assessment: Transit system officials reported conducting risk assessments that incorporate and combine all three elements of risk (threat, vulnerability, and consequence) to their systems and assets.	•	•	•

Source: GAO analysis of DHS and industry data.

^a Bullets in parentheses represent assessment information provided by TSA-TSNM-Mass Transit to DHS HITRAC for its risk analysis.

As table 1 shows, DHS developed the Strategic Homeland Infrastructure Risk Assessment (SHIRA) that assessed risk across 18 CI/KR sectors. To develop SHIRA, DHS collaborated with members of the intelligence community to determine threats against various systems and assets in the 18 CI/KR sectors. TSA then assessed the vulnerabilities and consequences that resulted from these threat scenarios and provided this information to HITRAC. Although TSA contributed to DHS's risk assessment effort, it has not conducted its own risk assessment of mass transit and passenger rail systems. TSA officials explained that the threat scenarios that SHIRA provided were general and not specific to mass transit and passenger rail. TSA could, however, use the information it provided for SHIRA to support a risk assessment.

Table 1 also shows that mass transit and passenger rail agencies, including Amtrak, have reported conducting risk assessments of their own systems. Officials from 26 of 30 of the transit systems we visited stated that they

had conducted their own assessments of their systems, including risk assessments. For example, one transit agency official stated that the agency had conducted risk assessments of its stations since 2003 and had updated them every 2 years. The official explained that his agency uses the risk assessment results to conduct cost benefit analyses that the agency uses before instituting new programs or purchasing equipment for its system. He also said that the assessments help the agency track risk reduction as a result of its security investments. Additionally, Amtrak officials stated that they conducted a risk assessment of all of their systems. As part of the assessment, Amtrak contracted with a private consulting firm to provide a scientific basis for identifying critical points at stations that might be vulnerable to IED attacks or that are structurally weak. Amtrak officials also stated that they gather and analyze threat information obtained from various classified and unclassified sources such as DHS, TSA, and the Federal Bureau of Investigation's Joint Terrorism Task Force. Transit agencies have also received assistance in the form of either guidance or actual risk assessments from several federal and industry stakeholders. Table 2 identifies the various assistance programs available to transit agencies for risk assessment efforts.

Table 2: Summary of Federal and Industry Stakeholders' Assistance to Transit Agencies for Risk Assessments Provided since 2004

DHS Transportation Security Administration (TSA)		
Office of Security Operations/ Surface Transportation Security Inspection Program (STSIP)	2008-present	Risk Assessment Tool: Mass transit and passenger rail risk assessment product to be used by TSA's surface inspectors. This tool is still being developed by the Office of Security Operations (OSO) in coordination with TSNM, TSA Office of Intelligence (TSA-OI), and STSIP. Initial field testing is estimated to commence in July 2009.
Transportation Sector Network Management (TSNM)/ Surface Transportation Security Inspection Program (STSIP)	2005-present	Security Analysis and Action Program (SAAP): Upon a transit agency's request, surface inspectors conduct analyses of a transit agency's critical infrastructure and physical systems and, among other things, identify deficiencies, determine the underlying causes, and develop recommendations to the agency to correct the deficiencies. As of November 2008, TSA had completed SAAPs for seven mass transit and passenger rail systems; however, no SAAP has been conducted since November 2008. ⁸
		Vulnerability Identification Self-Assessment Tool (VISAT): Self-assessment risk tool used by surface inspectors to conduct SAAP on transit agencies. The tool is to be used in developing a security baseline evaluation of a transit agency. The tool focuses on the prevention and mitigation of an array of threat scenarios and enables users to assess their security system's effectiveness in direct response to these specific threat scenarios.

DHS Federal Emergency Management Agency

Planning and Assistance Branch	2004-present	<p>Mass Transit Technical Assistance Program: FEMA officials, through a private consulting firm, assist passenger rail operators in enhancing their capacity and preparedness to respond to terrorist incidents and prioritize countermeasures. As of April 2009, FEMA has provided technical assistance to 36 passenger rail operators. This program was initially administered by DHS's Office of Domestic Preparedness (ODP) but has been managed by DHS-FEMA since March 2007.^b</p> <p>Transit Risk Assessment Methodology Tool Kit (TRAM): Risk guidance for transit agencies that was part of the Mass Transit Technical Assistance Program.</p>
--------------------------------	--------------	---

Department of Transportation (DOT)

Federal Transit Administration (FTA)	2004-present	Security and Emergency Management Technical Assistance Program (SEMTAP): Through this program, FTA officials provided guidance to the largest transit agencies on how to conduct threat and vulnerability assessments.
	2007	FTA-TSA Security and Emergency Management Action Items for Transit Agencies: Risk guidance for transit agencies including a resource link to a sample methodology.

Industry stakeholder

American Public Transportation Association (APTA)	2008-present	Recommended Practices for the Development and Implementation of a Security and Emergency Preparedness Plan (SEPP): Provides procedures for developing and implementing a security and emergency preparedness plan by transit agencies. Includes threat, vulnerability, and consequence identification and resolution approaches for transit agencies.
---	--------------	---

Source: GAO analysis of DHS, DOT and industry data.

Note: Although a few assistance programs started before 2004 (e.g., FEMA's Mass Transit Assistance Program and FTA's SEMTAP), for the purpose of this report, we are limiting our analysis to assistance that has been provided since 2004.

^a The seven SAAP assessments TSA reported conducting were those on the Virginia Railway Express, Portland Tri-Met Light Rail, Alaska Railroad, Amtrak Northeast Corridor power infrastructure, CSX Railroad (Indianapolis), Avon Yards (Indianapolis), and New Mexico Rail Runner Express.

^b In March 2004, the Secretary of Homeland Security consolidated ODP with the Office of State and Local Government Coordination to form the Office of State and Local Government Coordination and Preparedness (SLGCP). In 2007, SLGCP was incorporated under the DHS Preparedness Directorate as OGT and, in March 2007, OGT was incorporated into DHS-FEMA.

As table 2 shows, federal and industry stakeholders also provided assistance to transit agencies on how to assess risk. For example, FTA provided on-site technical assistance to the nation's 50 largest transit agencies (i.e., those transit agencies with the highest ridership) on how to conduct threat and vulnerability assessments, among other technical assistance needs, through its Security and Emergency Management

Technical Assistance Program (SEMTAP). According to FTA officials, although FTA continues providing technical assistance to transit agencies, the on-site SEMTAP program concluded in July 2006. Furthermore, FTA officials stated that on-site technical assistance was transferred to TSA when TSA became the lead agency on security matters for mass transit and passenger rail. Also, from 2004 through 2007, the former DHS Office of Domestic Preparedness (ODP), through a private consulting firm, provided assistance to transit agencies on how to conduct risk assessments through the Mass Transit Technical Assistance Program. Within this program, ODP developed a Transit Risk Assessment Methodology (TRAM) tool kit that provided transit agencies with an instrument to compare relative risks of terrorism against critical assets to better identify and prioritize security enhancements to reduce those risks. We reported in 2005 that officials from transit agencies participating in the Mass Transit Technical Assistance Program valued it and stated that the program was successful in helping them to devise risk-reduction strategies to guide security-related investments.²⁶ Subsequently, since the restructuring of ODP in 2007, this program has been transferred to FEMA's Planning and Assistance Branch where it has continued assisting transit agencies with risk assessments. However, according to FEMA's Chief of the Planning and Assistance Branch, because of the high cost of the program—\$300,000 to \$600,000 per transit agency—the rate of assistance to transit agencies has decreased annually. Also, FEMA is trying to convert the focus of the program from technical assistance to training. As such, FEMA plans to educate transit agencies on how to conduct risk assessments. Additionally, the same FEMA official reported that FEMA is also in the process of conducting a pilot project with one transit agency to evolve the program and the tool kit to an all hazards focus. Furthermore, recognizing the value of this program, officials from four of the 30 transit agencies we interviewed have since contracted with the same private consulting firm that ODP and FEMA used to update security plans or conduct a cost-benefit analysis of new programs or equipment.

Multiple Potential Threats to Mass Transit and Passenger Rail Have Been Identified

TSA has reported conducting annual threat assessments of the mass transit and passenger rail systems, and these assessments have provided TSA with an array of information about potential threats to the systems. TSA is responsible for conducting and issuing an annual threat assessment report for the mass transit and passenger rail systems. While it has been widely reported that no specific threats to the mass transit and passenger

²⁶ See [GAO-05-851](#).

rail systems currently exist, it has been noted that terrorists tend to target these systems, as overseas attacks on mass transit and passenger rail systems have demonstrated. TSA's Mass Transit Modal Annex identified numerous potential threats to mass transit, including placing a vehicle bomb near a station or track or introducing an IED or lower-yield explosive in a station, train, or bus, or laying explosives on a track. Deploying conventional or improvised explosives would likely result in scores of casualties. Since IEDs were used in the majority of the recent overseas attacks against mass transit and passenger rail systems, TSA and other experts are concerned that extremists may be motivated to employ similar tactics to target mass transit and passenger rail systems. In its Modal Annex, TSA also noted that the threat to heavy and commuter rail (i.e., underground, subway, elevated, rapid rail, or metro) is higher than the threat to buses and light rail (i.e., street cars, trolley) because of the accessibility of the large numbers of people typically found in the confined spaces of a rail system.

DHS Components, Including TSA, Conducted Several Vulnerability and Consequence Assessments That Identified Areas for Security Improvements

Several DHS components, including TSA, conducted assessments related to vulnerability and consequence since 2004, which have highlighted areas for security improvement. For example, DHS S&T conducted vulnerability assessments of transit tunnels as well as assessments of the potential consequences that various types of explosives threats would have on tunnel structures (which showed that improving evacuation plans and emergency response efforts, among other things, would improve public safety). Additionally, TSA has gathered vulnerability data through such programs as the Baseline Assessment for Security Enhancement (BASE). TSA officials reported that the BASE assesses the security posture of a mass transit or passenger rail system against the Security and Emergency Management Action Items and is TSA's primary source of vulnerability information.²⁷ For example, through initial assessments of the BASE program, TSA officials identified the need for increased security training at mass transit and passenger rail systems. Furthermore, FEMA has calculated consequence information for mass transit and passenger rail by using proxy data, such as population and national infrastructure indices. This information has been incorporated into the Transit Security Grant

²⁷ Security and Emergency Management Action Items consist of 17 action items developed by TSA and FTA which address current security threats and risks that confront transit agencies, with particular emphasis on priority areas where gaps need to be closed in security and emergency preparedness programs. Also, see appendix II for a list of these 17 action items.

TSA Reported Using Existing Assessments to Inform Its Security Strategy, but Its Approach Could Be Strengthened by Conducting a Risk Assessment

Program (TSGP).²⁸ TSA officials also reported using population density and ridership data as information for consequence assessments for mass transit and passenger rail systems and stated that they consider the number of potential casualties when determining consequence, and as a result, have chosen to focus their security efforts on the mass transit and passenger rail systems carrying the most passengers. Officials also mentioned that other factors such as the nature of the infrastructure (underground, underwater tunnels), time of day, and number of mass transit and passenger rail lines are also considered when assessing consequence.

TSA has used these various threat, vulnerability, and consequence assessments to inform its security strategy for mass transit and passenger rail—the Mass Transit Modal Annex. TSA reported that its efforts to inform its strategy included using information from TSA-OI’s annual mass transit threat assessment report to, for example, highlight the greater threats to underground and underwater passenger rail segments within a transit system. TSA also reported incorporating into its strategy information identified through its BASE reviews, such as the need for increased security training at mass transit and passenger rail systems.

While TSA reported using these various assessments to inform its mass transit and passenger rail security strategy, it could further strengthen its approach for securing these systems by combining the results from these assessments to conduct a risk assessment of the mass transit and passenger rail systems. Both the NIPP and TS-SSP establish a risk management framework that includes a process for considering threat, vulnerability, and consequence assessments together to determine the likelihood of a terrorist attack and the severity of its impact. The NIPP states that after the three elements of risk have been assessed, they are factored numerically and combined mathematically to provide an estimate of the expected loss considering the likelihood of an attack or other incident. It also states that when numerical values are not practical, scales could be used to estimate threat, vulnerability, and consequence. Thus, risk can be measured either quantitatively (i.e., numerically) or

²⁸ The TSGP provides grant funding to the nation’s key high-threat urban areas to enhance security measures for their critical transit infrastructure including bus, ferry and rail systems. For more information on the TSGP, please 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).

qualitatively (i.e., descriptively). However, rather than using the methodology established in the NIPP for assessing risk, TSA officials stated that the agency uses an intelligence-driven approach to make strategic investment decisions across the transportation system. Within this intelligence-driven approach for the sector, TSA also developed a tactical, threat-based process known as Objectively Measured Risk Reduction (OMRR) at the program level to help each of its individual divisions manage their day-to-day security operations. These approaches differ from the NIPP in part because they rely primarily on intelligence information to identify threats, prioritize tactics, and guide long-term investments, rather than systematically assessing the vulnerabilities and consequences of a range of threat scenarios.

In March 2009, we recommended that TSA work with DHS to validate its risk management approach by establishing a plan and time frame for assessing the appropriateness of TSA's intelligence-driven risk management approach for managing risk and document the results of this review once completed. TSA concurred with this recommendation.²⁹ TSA officials stated that they plan to revise and reissue the TS-SSP, as required by DHS, to reflect the adoption of their intelligence-driven methodology. As on June 2009, TSA reported that the update of the TS-SSP is ongoing, with the goal of completing the effort in 2009. Until TSA works with DHS to validate its risk management approach, TSA lacks assurance that its approach provides the agency and DHS with the information needed to guide investment decisions to ensure resources are allocated to the highest risks.

Moreover, as we reported in March 2009, although intelligence is necessary to inform threat assessments, it does not provide all of the information needed to assess risk, in particular information related to vulnerability and consequence assessments.³⁰ In addition, the intelligence-driven approach that TSA uses may be limited because, in contrast with practices adopted by the intelligence community, TSA officials do not plan to assign uncertainty or confidence levels to the intelligence information it uses to identify threats and guide long-range planning and strategic investment. Both Congress and the administration have recognized the

²⁹ GAO, *Transportation Security: Comprehensive Risk Assessments and Stronger Internal Controls Needed to Help Inform TSA Resource Allocations*, [GAO-09-492](#) (Washington, D.C., Mar. 27, 2009).

³⁰ [GAO-09-492](#).

uncertainty inherent in intelligence analysis and have required analytic products within the intelligence community to properly caveat and express uncertainties or confidence in analytic judgments. Furthermore, while intelligence can and does help the U.S. security community on an operational or tactical level, uncertainty in intelligence analysis limits its utility for long-range planning and strategic investment. Without expressing confidence levels in its analytic judgments, it will be difficult for TSA to correctly prioritize its tactics and long-term investments based on uncertain intelligence. In March 2009, we recommended that the Assistant Secretary of TSA work with the Director of National Intelligence to determine the best approach for assigning uncertainty or confidence levels to analytic intelligence products and apply this approach to intelligence products.

TSA officials agreed that they do not have a risk assessment and expressed the desire to conduct one; however, they reported that a lack of resources and other factors made completing a risk assessment challenging. For example, TSA officials stated that comprehensive vulnerability and consequence assessments are cost-prohibitive and time-intensive to conduct. Specifically, according to TSA officials, the Security Analysis and Action Program conducted by surface inspectors, a program that identifies, among other things, transit agencies' vulnerabilities can take days to complete resulting in a large resource investment. However, the 9/11 Commission Act requires TSA to use existing relevant assessments developed by federal and industry stakeholders, as appropriate, to develop a risk assessment for rail, including passenger rail. Furthermore, as suggested by the NIPP, agencies should consider existing risk measures when assessing risk. In addition to using the information for SHIRA, TSA could use other risk assessments, such as industry stakeholders' risk assessments and federal and industry stakeholders' guidance on how to conduct risk assessments, to potentially support a risk assessment of the mass transit and passenger rail systems.

Despite the challenges that TSA officials reported, it is important to note that risk assessment is an accepted and required practice with a long history of use in a wide variety of public and private sector organizations. Completing a risk assessment would provide TSA greater assurance that it is directing its resources toward mitigating the highest priority risks. Moreover, other agencies conduct risk assessments based on threat, vulnerability, and consequences and have overcome the challenges TSA

cited. For instance, within DHS, the U.S. Coast Guard, and FEMA use risk assessment methodologies to inform resource allocation.³¹

- The U.S. Coast Guard, which is responsible for securing the maritime transportation mode, conducts risk assessments using its Maritime Security Risk Analysis Model (MSRAM). Coast Guard units use the Maritime Security Risk Analysis Model to assess the risk of terrorist attack based on scenarios—a combination of target and attack mode—in terms of threats, vulnerabilities, and consequences to more than 18,000 targets. The model combines these assessments and provides analysis to identify security priorities and support risk management decisions at the strategic, operational, and tactical levels. The tool’s underlying methodology is designed to capture the security risks facing different types of targets spanning every DHS CI/KR industry sector, allowing comparison between different targets and geographic areas at the local, regional, and national levels. In conducting assessments, the Coast Guard Intelligence Coordination Center quantifies threat as a function of intent (the likelihood of terrorists seeking to attack), capability (the likelihood of terrorists having the resources to attack), and presence (the likelihood of terrorists having the personnel to attack).³² Intelligence Coordination Center officials stated that the Coast Guard uses MSRAM to inform allocation decisions, such as the local deployment of resources and grants.
- In June 2008, we reported that FEMA used a reasonable risk assessment methodology—based on a definition of risk as a function of threat, vulnerability, and consequence—to determine grant funding allocations under the Homeland Security Grant Program.³³ We found that this program utilized a reasonable methodology to assess risk and

³¹ In addition to the U.S. Coast Guard and FEMA, DHS’s Office of Science and Technology has conducted the following risk assessments using traditional methodologies: a Biological Threat Risk Assessment and an Integrated Chemical, Biological, Radiological, and Nuclear Terrorism Risk Assessment.

³² According to officials from the Intelligence Coordination Center, they use intelligence to quantify each sub-element within capability, intent, and presence. For example, presence is composed of two sub-elements—the number of known or suspected extremists and the number of areas of potential support or permissive environments—which are quantified and weighted within the overall threat model. This threat assessment is combined with assessments of vulnerability and consequence to produce MSRAM’s risk assessment.

³³ See GAO, *Homeland Security: DHS Risk-Based Grant Methodology Is Reasonable, But Current Version’s Measure of Vulnerability is Limited*, [GAO-08-852](#) (Washington, D.C.: June 27, 2008).

allocate grants to states and urban areas even though its assessment of vulnerability was limited. The risk assessment methodology used by FEMA is based on assessments of the threat, vulnerability, and consequence of a terrorist attack to each state and the largest urban areas. FEMA's methodology estimates the threat to geographic areas based on terrorists' capabilities and intentions, as determined by intelligence community judgment and data on credible plots, and planning and threats from international terrorist networks. Because this threat information is recognized as uncertain, threat accounts for 20 percent of the total risk to a geographic area, while vulnerability and consequence account for 80 percent.³⁴

Moreover, the NIPP states that implementing protective programs based on risk assessment and prioritization enables DHS, sector-specific agencies, and other security partners to enhance current CI/KR protection programs and develop new programs where they will offer the greatest benefit. By conducting a risk assessment, TSA would be able to better prioritize risks as well as more confidently assure that its programs are directed toward the highest priority risks.

³⁴ See [GAO-08-852](#). According to DHS officials, the agency's Office of Intelligence and Analysis (I&A) calculated the Threat Index by (1) collecting qualitative threat information with a nexus to international terrorism, (2) analyzing the threat information to create threat assessments for states and urban areas, (3) empanelling intelligence experts to review the threat assessments and reach consensus as to the number of threat tiers, and (4) assigning threat scores. This process, according to DHS officials, relied upon analytical judgment and interaction with the Intelligence Community, as opposed to the use of total counts of threats and suspicious incidents to calculate the Threat Index for the 2006 grant cycle. The final threat assessments are approved by the intelligence community—the Federal Bureau of Investigation, Central Intelligence Agency, National Counterterrorism Center, and the Defense Intelligence Agency—along with the DHS Under Secretary for Intelligence and Analysis and the Secretary of DHS, according to DHS officials.

TSA’s Security Strategy Could Be Strengthened by Including Key Characteristics of a Successful National Strategy and More Fully Addressing Elements Outlined in Executive Order 13416

TSA’s Mass Transit Modal Annex contains some information that is consistent with our prior work on characteristics of a successful national strategy and that is called for by Executive Order 13416: *Strengthening Surface Transportation Security*. However, the Modal Annex could be strengthened by including additional information that could help TSA and other implementing parties better leverage their resources to achieve the strategy’s vision of protecting mass transit and passenger rail systems from terrorist attacks. In February 2004, we identified six characteristics of successful national strategies.³⁵ Additionally, the Executive Order calls for the Secretary of Homeland Security to develop modal annexes for each transportation sector that includes certain elements, many of which are similar to the national strategy characteristics. Table 3 provides a brief description of five of the national strategy characteristics and relevant Executive Order elements that are discussed further below.³⁶

Table 3: Summary of Desirable Characteristics of Successful National Strategies and Related Executive Order Factors

Characteristic	Description
Purpose, scope, and methodology	Addresses why the strategy was produced, the scope of its coverage, and the process by which it was developed. In addition to describing what it is meant to do and the major functions, mission areas, or activities it covers, a national strategy would ideally also outline its methodology, such as discussing the principles or theories that guided its development, what organizations or offices drafted the document, whether it was the result of a working group, or which parties were consulted in its development.
Goals, subordinate objectives, activities, and performance measures	Addresses what the strategy is trying to achieve, steps to achieve those results, as well as the priorities, milestones, and performance measures to gauge results. At the highest level, a strategy could provide a description of an ideal “end state,” followed by a logical hierarchy of major goals, subordinate objectives, specific activities, and performance measures to achieve results. ^a Executive Order 13416 calls for the annex of each transportation mode, or Modal Annex, to identify processes for assessing compliance with security guidelines and requirements, and for assessing the need for revision of such guidelines and requirements to ensure their continuing effectiveness—something that could be accomplished with defined performance measures. The Order also directs TSA to evaluate the effectiveness and efficiency of current surface transportation security initiatives and calls for the annex to identify processes for assessing compliance with security guidelines and requirements.

³⁵ [GAO-04-408T](#).

³⁶ The sixth characteristic is “Problem Definition and Risk Assessment,” which addresses the particular national problems and threats the strategy is directed toward. However, because we provided details earlier in our report in the section on risk assessment, we do not address this characteristic in this section of our report.

Characteristic	Description
Resources, investments, and risk management	Addresses what the strategy will cost, the sources and types of resources and investments needed, and where resources and investments should be targeted based on balancing risk reductions with costs. Ideally, a strategy would also identify criteria and appropriate mechanisms to allocate resources, such as grants, in-kind services, loans, and user fees, based on identified needs. Alternatively, the strategy might identify appropriate “tools of government,” such as regulations, tax incentives, and standards; or stimulate nonfederal organizations to use their unique resources.
Organizational roles, responsibilities, and coordination	Addresses which organizations are to implement the strategy, their roles and responsibilities, and mechanisms for collaboration. This information considers who is in charge, not only during times of crisis but also during all phases of combating terrorism, including prevention, vulnerability reduction, and response and recovery. This entails identifying the specific federal entities involved and, where appropriate, the different levels of government or stakeholders, such as state and local governments and private entities. Executive Order 13416 also calls for the Secretary of Homeland Security to develop modal annexes that include a description of the respective roles, responsibilities, and authorities of federal, state, local, and tribal governments. A strategy could also describe the organizations that will provide the overall framework for accountability and oversight, and identify specific processes for collaboration and address how any conflicts would be resolved.
Integration and implementation	Addresses how a national strategy relates to other strategies’ goals, objectives, and activities and to subordinate levels of government and their plans to implement the strategy. For example, a national strategy could discuss how its scope complements, expands upon, or overlaps with other national strategies. Also, related strategies could highlight their common or shared goals, subordinate objectives, and activities. Executive Order 13416 requires that the modal annex identify existing security guidelines and requirements. A strategy could address its relationship to other agency strategies using relevant documents from implementing organizations, such as strategic plans, annual performance plans, or annual performance reports that the Government Performance and Results Act of 1993 requires of federal agencies. A strategy might also discuss, as appropriate, various strategies and plans produced by the state, local, or private sectors and could provide guidance, for example, on the development of national standards, to more effectively link the roles, responsibilities, and capabilities of the implementing parties.

Source: GAO.

^aA goal (also known as a strategic goal or objective) constitutes a specific set of policy, programmatic, and management objectives for the programs and operations covered in the strategic plan, and serves as a framework from which the annual objectives and activities are derived. A goal is expressed in a manner that allows a future assessment to be made regarding whether the goal was or is being achieved. Subordinate objectives assist in focusing the mode’s programs and activities to meet the goals. Activities are specific programs and actions to achieve the subordinate objectives. Performance measures are particular values or characteristics used to measure output or outcome of activities, objectives, and goals. An outcome measure describes the intended result or effect from carrying out a program or activity. It defines an event or condition that is external to the program or activity and that is of direct importance to the intended beneficiaries and/or the public. An output measure describes the level of activity that will be provided over a period of time, including a description of the characteristics (e.g., timeliness) established as standards for the activity.

The Modal Annex contains information related to three of the characteristics we identified as desirable characteristics for a successful national strategy: (1) purpose, scope and methodology; (2) organizational roles, responsibilities, and coordination; and (3) integration and implementation. For example, the organizational roles, responsibilities, and coordination characteristic, which is also an element in Executive Order 13416, calls for agencies to identify which organizations are to implement the strategy, their roles and responsibilities, and the

mechanisms for collaborating.³⁷ The Modal Annex generally addresses this characteristic as it identifies relevant stakeholder roles and responsibilities. Specifically, the Modal Annex states that TSA has primary responsibility for ensuring security for mass transit and passenger rail while other federal and industry stakeholders, such as the FTA, FRA, FBI, private sector, and transit labor representatives have partnership roles. The Modal Annex also describes stakeholders' collaboration efforts. For example, it describes FTA, FRA, APTA, and transit operators' involvement in the development and implementation of security standards and directives. See appendix III for more information on the characteristics the Modal Annex includes.

The Modal Annex, however, could be strengthened by addressing the other two desirable characteristics of an effective national strategy: (1) goals, subordinate objectives, activities, and performance measures and (2) resources and investments. Both of these could be useful in achieving the vision articulated in the Modal Annex of securing the mass transit and passenger rail systems.

Goals, Subordinate Objectives, Activities, and Performance Measures

In conformance with this characteristic, the Modal Annex identifies sector-wide goals that apply to all modes of transportation as well as subordinate objectives specific to mass transit and passenger rail systems. For instance, one of TSA's transportation sector goals is to enhance resiliency of the U.S. transportation system and presents three subordinate objectives to demonstrate how the agency intends to meet this goal. Further, for each subordinate objective, TSA presents information to explain what TSA, other federal components, or industry stakeholders are doing to meet the subordinate objective. For example, the agency identifies its Explosives Detection Canine Teams as an activity to accomplish assessing, managing, and reducing risk associated with key modes, links, and flows within critical transportation systems. Table 4

³⁷ This information helps answer the fundamental question about who is in charge, not only during times of crisis, but also during all phases of homeland security and combating terrorism including prevention, vulnerability reduction, and response and recovery. This entails identifying the specific federal entities involved and, where appropriate, the different levels of government or stakeholders, such as state and local governments and private entities. In our past work, we found that a successful strategy clarifies implementing organizations' relationships in terms of leading, supporting, and partnering. In addition, a strategy could describe the organizations that will provide the overall framework for accountability and oversight. Furthermore, a strategy might identify specific processes for collaboration between sectors and organizations—and address how any conflicts would be resolved.

provides a complete list of the TSA’s goals and their subordinate objectives for the mass transit and passenger rail systems.

Table 4: Sector Goals and Passenger Rail and Mass Transit Subordinate Objectives to Complete Sector Goals

Sector Goal	1) Prevent and deter acts of terrorism using or against the transportation system
Subordinate Objectives	<ul style="list-style-type: none"> • Implement risk-based, flexible, layered and unpredictable security programs. • Increase vigilance of travelers and transportation workers. • Enhance information and intelligence sharing among transportation sector security partners.
Sector Goal	2) Enhance resiliency of the U.S. transportation system
Subordinate Objectives	<ul style="list-style-type: none"> • Assess, manage, and reduce risk associated with key nodes, links, and flows within critical transportation systems. • Ensure the capacity for rapid response and recovery to all-hazards events. • Develop, disseminate, and promote the adoption of a standard risk reduction methodology.
Sector Goal	3) Improve the cost-effective use of resources for transportation security
Subordinate Objectives	<ul style="list-style-type: none"> • Align sector resources with the highest priority transportation security risks using both risk and economic consequences as decision criteria. • Maximize passenger rail and mass transit sector participation as a partner in the developing and implementing of public sector programs for critical infrastructure/key resource protection. • Improve transportation sector security research, development, test, and evaluation resource allocation. • Ensure that public sector funds expended have achieved the expected risk reduction.

Source: GAO Analysis of TSA information.

While the Modal Annex identifies goals, objectives, and activities, it does not contain measures or targets on the effectiveness of the operations of the security programs identified in the Modal Annex. For example, one of TSA’s security programs listed in the Modal Annex—Security Technology Deployment—aligns under one of the sector goals: prevent and deter acts of terrorism using or against the transportation system. However, the Modal Annex contains no measures or targets to assess the effectiveness of this program in achieving this goal. In August 2006, we reported that performance measures are an important tool to communicate what a program has accomplished and provide information for budget decisions. Further, we noted that it is desirable for these measures to be as effective as possible in helping to explain the relationship between resources expended and results achieved because agencies that understand this

linkage are better positioned to allocate and manage their resources effectively.³⁸

Although the Modal Annex does not contain specific measures or targets, it does call for developing measures of effectiveness to evaluate mass transit and passenger rail efforts to mitigate risk and increase the resilience of systems and assets. TSA has developed performance measures to track the progress that the surface transportation security program has made in conducting activities to enhance the security of the mass transit and passenger rail systems. Specifically, TSA's Surface Transportation Security Inspection Program fiscal year 2009 Annual Inspection Plan identifies annual and quarterly performance metrics for conducting mass transit and passenger rail-related assessments that TSA plans nationwide:

- number of inspections conducted per 1,000 inspector work hours on mass transit, passenger rail, and freight rail systems and³⁹
- number of BASE reviews conducted at the top 100 largest transit agencies.

While these measures are useful in tracking activities or actions taken, they are output measures that do not fully inform TSA about how various actions have impacted the security of mass transit and passenger rail systems' goals and objectives. For example, TSA has so far reported the progress in its Visible Intermodal Prevention and Response (VIPR) program in terms of the number of VIPR operations TSA conducted, but has not yet developed measures or targets to report on the effectiveness of

³⁸ GAO, *Coast Guard: Non-Homeland Security Performance Measures Are Generally Sound, but Opportunities for Improvement Exist*, [GAO-06-816](#) (Washington, D.C.: Aug. 16, 2006).

³⁹ According to TSA's fiscal year 2009 Regulatory Inspection Plan, this measure demonstrates the efficiency of inspection activities by quantifying the number of completed mass transit and freight rail inspections. For mass transit and passenger rail, this includes BASE reviews and station profiles, and for freight rail, this includes Security Action Item Reviews.

the operations themselves.⁴⁰ However, in June 2009, TSA program officials reported that they are planning the introduction of additional performance measures for no later than the first quarter of fiscal year 2010. These measures would gather information on (1) interagency collaboration by collecting performance feedback from federal, state and local security, law enforcement, and transportation officials prior to and during VIPR deployments; and (2) stakeholder views on the effectiveness and value of the VIPR deployment.

In February 2009, TSA reported plans to introduce its first outcome measures for its mass transit and passenger rail security programs. For example, TSA plans to introduce a performance measure for its BASE review program. TSA officials reported that they plan to calculate this measure by comparing the results from the first and second round BASE reviews for the nation's top 100 largest transit mass transit and passenger rail systems. TSA also reported plans to introduce additional outcome performance measures in the future, including an overall risk reduction measure tied to the BASE program. Implementing these new performance measures and including them in future updates of the Mass Transit Modal Annex should better inform decision makers at TSA on the effect of its programs in securing mass transit and passenger rail.

Resources and Investments

While the Modal Annex identifies how TSA has allocated funds available to different transit agencies, the Modal Annex provides relatively few details on how grant resources should be targeted. Also, the Modal Annex contains little information on resources and costs associated with mass transit and passenger rail security programs. For example, the Modal Annex identifies as its third sector-goal, as shown on table 4, improve the cost-effective use of resources for transportation security; however, it provides few details on the costs, types, or levels of resources associated with implementation of the security programs that are aligned with this goal. Furthermore, the Modal Annex describes risks to the mass transit and passenger rail systems by discussing overseas attacks and the

⁴⁰ Since late 2005, TSA has reported deploying Visible Intermodal Prevention and Response (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.

potential consequences of such attacks in the United States. However, the Modal Annex does not provide information on the cost of the consequences of such attacks and is silent on risk assessment efforts. TSA officials acknowledged the lack of this information and the need to include it in future updates of the Modal Annex. While providing cost estimates may be difficult to do, including resources and costs, to the extent possible, would help implementing parties allocate budgets according to priorities and constraints, and would help stakeholders shift such investments and resources as appropriate.

Federal and Industry Stakeholders Have Taken Key Actions to Strengthen Transit Security and Federal Actions Have Been Generally Consistent with TSA's Strategy, but Opportunities Exist to Strengthen Some Programs

Since 2004, federal and industry stakeholders have implemented several key actions to strengthen the security of the nation's mass transit and passenger rail systems and federal actions have generally been consistent with TSA's security strategy. However, federal efforts are largely in the early stages and opportunities exist for TSA to strengthen some programs.

Federal Actions to Secure Mass Transit and Passenger Rail Have Been Varied and Generally Consistent with TSA's Security Strategy

Since 2004, federal stakeholders have taken a number of key actions to secure mass transit and passenger rail systems and TSA has been the primary federal agency involved in implementing these actions. In general, these actions can be categorized into three areas: (1) deploying surface inspectors and other personnel to conduct voluntary security assessments and security operations at the nation's largest mass transit and passenger rail systems; (2) establishing and implementing coordination mechanisms between federal entities and mass transit and passenger rail industry stakeholders; and (3) coordinating with the DHS Science and Technology Directorate (DHS S&T) to develop and test new

security technology appropriate for deployment in mass transit and passenger rail systems.⁴¹

Since 2004, TSA's primary security activity for mass transit and passenger rail has been conducting voluntary security assessments of the nation's top 100 largest mass transit and passenger rail systems through its BASE program.⁴² TSA has used the BASE results to inform the development of security enhancement programs and to determine priorities for allocating mass transit and passenger rail security grants. In addition, through its VIPR program and its National Explosive Detection Canine Team Program (NEDCTP), TSA has deployed personnel and explosive detection canine teams to augment mass transit and passenger rail systems' security forces to conduct hundreds of random and event-based security operations as a show of force to deter potential terrorist attacks at key mass transit and passenger rail stations.

Federal agencies have taken other actions as well to strengthen security by enhancing coordination with transit industry stakeholders. For example, TSA established the monthly Transit Policing and Security Peer Advisory Group (PAG) and FTA initiated the semi-annual Transit Safety and Security Roundtables, both of which provide forums for TSA and mass transit and passenger rail systems, including Amtrak, to share security information and ideas. Additionally, FTA has enhanced mass transit and passenger rail security by funding the development and delivery of security training curriculum and programs for mass transit and passenger rail system employees, and by developing a list of recommended security and emergency action items for mass transit security programs, which it later updated in collaboration with TSA. TSA also collaborates with DHS S&T to pursue research, development, and testing of new security technology appropriate for deployment in mass transit and passenger rail systems. In 2006, DHS reorganized its security technology research and development structure, and under the new structure, TSA is to identify technology priorities to address security gaps and communicate these priorities to DHS S&T, which in turn is to conduct technology research,

⁴¹ Another key action TSA has taken to strengthen mass transit and passenger rail security since 2004 has been providing grant funding through the Transit Security Grant Program (TSGP). We reported on DHS's administration of the grant program in [GAO-09-491](#).

⁴² From August 2006 to February 2009, TSA reported conducting BASE reviews of 82 of the top 100 largest mass transit and passenger rail systems. As of February 2009, five transit agencies had declined TSA's request to participate in the reviews.

development, and testing. Table 5 provides descriptions of key federal programs and activities, initiated since 2004, mostly by TSA and FTA, to enhance mass transit and passenger rail system security. For a more extensive list of federal programs and activities, see appendix IV.

Table 5: Key Federal Actions Taken to Enhance Mass Transit and Passenger Rail Security Since 2004

Category/Program	Lead agency	Description
<i>Deploying manpower</i>		
Surface Transportation Security Inspection Program (STSIP)	TSA	Established in 2005, TSA's surface inspectors serve as the agency's field force for conducting non-regulatory security assessments, outreach, and technical assistance with the nation's top 100 largest mass transit and passenger rail agencies, as well as participating in VIPR security operations at key transit and passenger rail locations. TSA reported that, as of February 2009, its surface inspectors had conducted non-regulatory security posture assessments—or BASE reviews—of 91 mass transit and passenger rail agencies, including 82 of the largest agencies, and had conducted over 1,350 site visits to mass transit rail stations to complete Station Profiles, which gather detailed information on a station's physical security elements, geography, and emergency points of contact.
Visible Intermodal Prevention and Response (VIPR) Program	TSA	Since late 2005, TSA has reported deploying over 800 teams of 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 stations, and passenger and baggage screening operations using specially trained behavior detection officers and explosive detection canine teams and explosive detection technologies.
National Explosive Detection Canine Team Program (NEDCTP)	TSA	TSA implemented the NEDCTP in 2000 for aviation, and in 2005 expanded the program into mass transit and passenger rail. TSA has worked in partnership with transit systems to procure, train, certify, and deploy 88 explosives detection canine teams to 15 participating mass transit and passenger rail systems nationwide to provide mobile and flexible deterrence and explosives detection capabilities. TSA provides the canine training for the handler and the dogs and also allocates funds to cover the costs associated with continued training and maintenance of the capabilities of the team, while the transit system commits a handler to attend the TSA training and receive program certification.
<i>Coordinating with federal and industry stakeholders and issuing guidance</i>		
DHS/DOT memorandum of understanding (MOU) for coordination of roles/responsibilities	TSA FTA	Through a 2004 MOU and 2005 annex DOT (FTA) and DHS (TSA) agreed to closely coordinate their mass transit and passenger rail programs and services in developing transit security guidance and regulations. The agreements confirm that TSA has the lead role for transportation security and DOT has a supporting role in providing technical assistance and with assisting DHS in implementation of its security policies.

Category/Program	Lead agency	Description
Transit, Commuter and Long Distance Rail Government Coordinating Council (GCC) and Mass Transit Sector Coordinating Council (SCC) Joint Working Groups	TSA FTA	In 2007, under the Transit, Commuter and Long Distance Rail Government Coordinating Council (GCC) and Mass Transit Sector Coordinating Council (SCC) framework, TSA and FTA collaborated with the American Public Transportation Association to establish working groups composed of federal and industry mass transit and passenger rail security stakeholders to serve as a modal coordinating council for mass transit and passenger rail systems. Working groups were established in three substantive areas: security training, security technology, and grants.
Transit Policing and Security Peer Advisory Group (PAG)	TSA	In late 2006, TSA established the monthly Transit Policing and Security Peer Advisory Group (PAG) to bring together 16 transit police chiefs and security directors from Amtrak and major transit systems across the nation to act as a consultative forum for advancing the security concerns of transit systems.
Transit Safety and Security Roundtables	TSA FTA	Administered in 2003 and 2004 by FTA and jointly administered since 2005, TSA and FTA have convened semi-annual Transit Safety and Security Roundtables to serve as a means for representatives of the 50 largest mass transit agencies to share security-related ideas and information.
Security Standards	TSA FTA	In accordance with the DOT/DHS MOU annex, FTA is leading an initiative with TSA to develop security standards for mass transit and passenger rail systems, with a focus on recommended procedures and practices. FTA has funded APTA to administer this initiative, and as of March 2009, APTA had issued six security standards related to security emergency management, security infrastructure, and security risk management.
<i>Developing security technology and providing technology information</i>		
Security technology research and development (R&D)	DHS S&T/ TSA	DHS S&T and TSA collaborate 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.
Transportation Research Board	FTA	FTA sponsors academic research from the Transportation Research Board (TRB) which is one of six divisions within the National Research Council. The National Research Council serves as an independent adviser to the federal government and others on scientific and technical questions of national importance. TRB has produced several reports on public transportation security, such as a report on mass transit passenger security inspections procedures and technology.

Source: GAO analysis of TSA and FTA programs.

Federal Mass Transit and Passenger Rail Security Actions Are Generally Consistent with TSA's Security Strategy

Federal actions to secure mass transit and passenger rail systems generally have been consistent with those that TSA outlined in its security strategy for mass transit, the Mass Transit Modal Annex. The Modal Annex describes TSA's strategic objectives and associated federal programs and activities to meet these objectives. For example, one objective calls for conducting security readiness assessments, which TSA has been doing since August 2006 through its BASE review program. Another objective calls for a public awareness program, which TSA reported implementing

through its Employee Awareness Poster Program.⁴³ See appendix V for a list of all of the Modal Annex mass transit objectives and TSA's reported actions to achieve these objectives.

Mass Transit and Passenger Rail Systems Have Taken Key Actions to Enhance Security

Mass transit and passenger rail systems, including Amtrak, reported taking key actions since 2004 to improve their security. Most systems reported making operational enhancements to their security programs, such as adding security personnel or transit police. Moreover, some of the largest systems have implemented varying types of random passenger or baggage inspection screening programs. These programs include deploying security personnel at checkpoints to conduct visual observation of passengers for suspicious behaviors as well as non-invasive baggage checks. Since 2004, Amtrak reported taking additional actions to secure its system, focusing particularly on securing stations on its Northeast Corridor. Among other things, Amtrak introduced new passenger and baggage screening operations, increased its own explosive detection canine capacity, and deployed an armed mobile tactical team to respond to threats and conduct deterrent operations. Further, Amtrak provided security training to all of its frontline employees and conducted additional security risk assessments on its system as the baseline for developing its corporate security strategy.

Officials from 24 of 25 passenger rail systems we interviewed and Amtrak also reported taking actions to strengthen the security of their systems in response to TSA's 2004 passenger rail security directives. These actions included removing trash receptacles from high-risk platform areas and deploying explosive detection canine units to patrol their systems. Amtrak also initiated identification checks for adult passengers. However, TSA's security directives contained limited requirements for passenger rail, and

⁴³Through the Employee Awareness Poster Program, TSA partners with mass transit and passenger rail agencies to produce tailored posters specifically focused on transit employee security awareness. TSA develops a common theme, transit agencies provide graphics, logos, and quotations, and TSA tailors the posters for use by the transit agencies.

TSA has not enforced their implementation.⁴⁴ Additionally, TSA released a report summarizing results of the BASE reviews it had conducted of mass transit and passenger rail systems during fiscal year 2007.⁴⁵ This report showed that almost all transit agencies reported providing some type of security training to their frontline employees; however, the extent of the training provided varied greatly—with a majority providing an introductory level of safety and security training for new hires, but not refresher training.⁴⁶

Many mass transit and passenger rail agencies also reported making capital improvements to secure their systems. For example, since 2004, 19 of the 30 transit agencies we interviewed had embarked on programs 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. For bus transit agencies, capital improvements have included installing automatic vehicle location tracking, silent alarms, and engine disabling systems to counter potential hijacking threats.

⁴⁴ On May 20, 2004, TSA issued Transportation Security Directives RAILPAX 04-01: Threat to Passenger Rail Systems and RAILPAX 04-02: Threat to Passenger Rail Systems—National Railroad Corporation (Amtrak) and Alaska Rail Road Corporation. As of March 2009, these directives remained in place. However, senior TSA Headquarters officials told us that since 2006, as a matter of policy, TSA had chosen not to enforce industry compliance with the directives, and instead used the security directives as a tool to communicate general security priorities. TSA officials attributed their decision not to enforce the directives to passenger rail industry concerns regarding the impracticality of implementing some of the measures, the ambiguity of the directives, and the lack of industry input in developing and issuing the directives. Of the 30 systems which we included in our study, 25 systems operated passenger rail services and were subject to implementing the security directives.

⁴⁵ In fiscal year 2007, TSA reported conducting BASE reviews of 53 mass transit and passenger rail systems, including 44 that were ranked in the top 50 in the nation based on ridership. TSA's BASE review report assessed the status of these 53 systems in implementing the 17 TSA/FTA Security and Emergency Management Action Items.

⁴⁶ According to the 9/11 Commission Act, frontline transit employees include an employee of a public transportation agency who is a transit vehicle driver or operator; dispatcher; maintenance and maintenance support employee; station attendant; customer service employee; security employee; or transit police or any other employee who has direct contact with riders on a regular basis, and any other employee of a public transportation agency that the Secretary determines should receive training. Pub. L. No. 110-53, § 1402(4), 121 Stat. 266, 401 (2007).

While mass transit and passenger rail systems as a whole have taken actions to enhance their security, TSA's BASE reviews indicated that rail transit agencies were implementing a wider range of security programs than bus only transit agencies.⁴⁷ For example, according to TSA's initial findings from its BASE reviews of the 50 largest transit agencies, conducted during fiscal year 2007, rail transit agencies implemented more of the TSA/FTA security and emergency management action items than bus-only systems. TSA officials attributed the differences to three factors. First, passenger rail agencies have been required to comply with FTA's triennial State Safety Oversight audits that require passenger rail agencies to have both a safety and security plan in place and TSA's 2004 security directives. In contrast, bus-only transit agencies have not been required to implement such FTA security requirements, and no federal agency has issued bus-specific security requirements or directives. Second, bus-only transit agencies tend to be smaller than rail only or rail and bus transit agencies and have fewer financial resources available to invest in security activities. Finally, because passenger rail has been the target of recent high profile terrorist attacks overseas and rail is considered a higher security risk to terrorist attack than bus-only systems, passenger rail transit security has received greater focus—both by the transit industry and the federal government.

⁴⁷ Rail transit agencies include either (1) those which operate passenger rail systems only or (2) a combination of both passenger rail and bus transit systems.

Opportunities Exist for TSA to Strengthen Management and Coordination of Three Mass Transit and Passenger Rail Security Programs

DHS is Exploring New Security Technologies, but Expanding Outreach and Improving Information Sharing Could Strengthen Future Research and Development Endeavors

As part of its research and development (R&D) strategy, DHS has been exploring new explosive detection technologies, particularly those that deter, detect, defeat, and protect against the use of IEDs in or around transit infrastructure. Accordingly, DHS technology pilot projects for mass transit and passenger rail have sought to identify and develop technologies that can effectively detect explosive weapons or compounds while causing minimal delays to passengers, such as fare card vending machines capable of detecting explosive residue on passengers' bodies or bags (see figure 3). Although DHS has worked to develop some security technologies specific to mass transit and passenger rail systems, most technologies that it has pursued could work across different transportation modes, including aviation, maritime, mass transit, and passenger rail. DHS has also pursued several infrastructure protection projects that address the threat of IEDs, with a particular focus on addressing the vulnerabilities of underground and underwater transit tunnels. Unlike its role in commercial aviation, TSA does not procure or deploy security technologies for mass transit and passenger rail systems. Instead, TSA partners with mass transit and passenger rail systems to conduct pilot projects and demonstrations of commercially available technologies and technologies from DHS laboratories. The mass transit and passenger rail systems themselves determine which security technologies to procure and deploy.⁴⁸ See appendix VI for a list of ongoing and completed TSA and DHS mass transit and passenger rail security-related technology pilot programs.

⁴⁸ TSA conducts this work through the Surface Transportation Technology Program, established in fiscal year 2007. It conducts this work to assess potential technologies for addition to the Transit Security Grant Program guidance, to gain a better understanding of emerging technologies, to evaluate technologies in the mass transit environment, and to provide test results and lessons learned to mass transit and passenger rail authorities.

Figure 3: Photo of DHS S&T Pilot Technology for a Fare Card Vending Machine with Explosive Trace Detection Capability



Source: DHS Science and Technology Directorate.

A 2006 pilot test by DHS S&T involved a fare card vending machine capable of detecting trace amounts of explosives residue on the fingertips of passengers. Though successfully demonstrating the technology, the machines were estimated to cost 75 to 100 percent more than standard fare-card vending machines.

Since 2007, TSA, like other DHS components, has been responsible for articulating the technology needs of all transportation sector end-users—including mass transit and passenger rail agency operators—to DHS S&T for development.⁴⁹ TSA has taken some initial actions to reach out to mass transit and passenger rail systems regarding their security R&D needs;

⁴⁹ To carry out this process, DHS S&T brings together agency representatives into Integrated Product Teams (IPTs) to collaboratively set research and spending priorities to the individual project level. The IPTs do not include technology end-users—such as transit bus and rail system security operators—because DHS has assumed that its component agencies would represent end-user interests.

however, these efforts could be expanded and improved by more fully leveraging existing forums to solicit a wider range of input. This effort is important because, as we reported in September 2004, stakeholders are more likely to use research results if they are involved in the R&D process from the beginning.⁵⁰ The Mass Transit Modal Annex states that DHS S&T and TSA will identify security technology needs in full partnership with the mass transit community. To achieve this, TSA officials told us that TSA leverages existing forums for communication, such as the semi-annual Transit Security Roundtables, to identify technology capability gaps and to solicit input and feedback on its technology priorities. Additionally, in 2008, TSA headquarters officials reported that they sought input from transit industry representatives through the Transit Policing and Security Peer Advisory Group and the Mass Transit Sector Coordinating Council Security Technology Working Group. Nonetheless, in a September 2008 draft report, the Mass Transit Sector Coordinating Council Security Technology Working Group reported that other than occasional telephone discussions, there was no ongoing structure that brought the federal government and transit industry together to discuss transit security technology priorities, needs, and areas of potential interest for technology advancement and research.⁵¹ In September 2004, we recommended that DHS and TSA improve their outreach to the transportation industry (including mass transit and passenger rail systems) to ensure that the industry's R&D security needs have been identified and considered. DHS agreed that this recommendation was key to a successful R&D program and since that time, DHS and TSA have made some preliminary efforts to outreach on R&D security issues.⁵² However, by continuing to expand these efforts and getting input early on in the project selection process,

⁵⁰ GAO, *Transportation Security R&D: TSA and DHS Are Researching and Developing Technologies, but Need to Improve R&D Management*, [GAO-04-890](#) (Washington D.C.: Sept. 30, 2004).

⁵¹ There are two working groups comprised of federal, industry, and other stakeholders for transportation security research and development. The Mass Transit Sector Coordinating Council (SCC) Security Technology Working Group is led by the American Public Transportation Association (APTA). This group provides recommendations to federal stakeholders in the area of security technology R&D. The Transportation Systems – Sector Specific Plan Research and Development Working Group meets on a monthly basis and is working on ways to harmonize the R&D efforts for critical infrastructure in all transportation sectors by identifying currently available technology and facilitating common definitions and standards, among other activities.

⁵² [GAO-04-890](#).

TSA should be able to ensure that DHS has adequately considered and addressed the full scope of the industry's R&D needs.

TSA has taken initial actions to share information on available security technologies, but could strengthen its approach by providing more information to support transit agencies that are considering deploying new security technologies. 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.⁵³ 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. These officials said that they did not use HSIN when considering such investments because HSIN did not contain product details that would support these decisions, including details on product capabilities, maintenance, ease of use, and the suitability of the products in a bus or rail venue. We reviewed HSIN and found that for a given security product, TSA's listing provides a categorical definition (such as video motion analysis), a sub-category (such as day/night camera), and the names of products within those categories. However, HSIN neither provides nor indicates how transit agencies can obtain information beyond the product's name and function. A senior program official with TSA's TSNM mass transit division told us that mass transit and passenger rail system officials would already know whom to contact at TSA for more information on a product. However, the official acknowledged that the product listing could be enhanced by including the contact information of the TSA officials capable of providing that information. In the absence of more detailed information on security-related technologies, officials from 19 of 30 mass transit and passenger rail systems we interviewed told us that they either (1) asked other operators

⁵³ In September 2005, we recommended that DHS and TSA consider establishing an online clearinghouse of information on security-related products, such as closed circuit television cameras or intrusion detection systems. In December 2002, we also reported that the federal government should play a greater role in testing transportation security technology and making this information available to industry stakeholders. See [GAO-05-851](#) and [GAO, *Mass Transit: Federal Action Could Help Transit Agencies Address Security Challenges*, GAO-03-263](#), (Washington D.C.: Dec. 13, 2002).

about their experiences with a particular technology; (2) performed their own research via the Internet or trade publications; or (3) performed their own testing. Making the results of research testing available to industry stakeholders could be a valuable use of federal resources by reducing the need for multiple industry stakeholders to perform the same research and testing.

The senior TSA program official with the TSNM mass transit division also acknowledged that HSIN contained limited technology information but noted that the site's content was largely in the early stages of development. The official attributed some of the limitations to TSA's reluctance to provide substantive details regarding any particular product, since TSA officials did not want to be perceived as endorsing any particular vendor. Nonetheless, 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. Although TSA has set this goal for HSIN, there was no set deadline for the content-related improvements. 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.

TSA Reported Taking Steps to Respond to Transit Industry Concerns and Improve the Effectiveness of its VIPR Program

In response to mass transit and passenger rail industry concerns about its VIPR program, TSA reported taking steps to work with the industry to improve the effectiveness of the program. TSA conducts VIPR operations as a way to introduce security measures (such as random bag searches) at mass transit and passenger rail systems to deter potential terrorist threats, augment local security forces, and promote the visibility of TSA resources.⁵⁴ TSA, to date, has conducted over 800 VIPR operations at mass transit and passenger rail systems. TSA also reported that almost all operations were deployed on a random basis or to enhance security at

⁵⁴ VIPR teams consist of varying sizes and composition of TSA personnel and other federal, state, or local assets. TSA has designated Federal Air Marshals (FAMs)—the primary law enforcement entity within TSA, whose primary mission is protecting air passengers and crew—as the lead for coordinating VIPR operations. Other VIPR personnel may include Surface and Aviation Transportation Security Inspectors, explosive detection canine teams, and behavioral detection officers—personnel trained to screen for high-risk individuals based on involuntary physical or psychological behavior.

special events or on holidays, rather than in response to specific threat information.⁵⁵

Mass transit and passenger rail system officials we interviewed had varying opinions on the effectiveness of the VIPR operations that TSA had conducted on their systems. For example, security and management officials from 5 of the 30 mass transit and passenger rail systems we visited told us that they generally welcomed the additional security resources that the VIPRs provided. In contrast, officials from four other mass transit and passenger rail systems reported that because they were already deploying their own transit police and security personnel on their systems on a daily basis, the addition of a largely unarmed VIPR team on a single day did not add significant security value especially with the additional planning and costs incurred by these operations.

In response to VIPR planning and implementation concerns raised by large mass transit and passenger rail systems, in October 2007 TSA issued a Concept of Operations (CONOPS) for its VIPR program that established general guidelines for the planning and execution of a VIPR deployment. TSA developed the guidance in coordination with members of the Transit Policing and Security Peer Advisory Group and issued the guidance to both its field personnel and the mass transit industry. The CONOPS includes general guidelines for 10 core components of collaboration, such as coordination, planning, and communications.⁵⁶ In June 2008, the DHS Inspector General (DHS-IG) reported on VIPR planning and implementation concerns and noted that transit system officials reported that TSA's issuance of the VIPR guidance had led to improvements that addressed many of the VIPR implementation concerns.⁵⁷ Nevertheless, our

⁵⁵ TSA program officials reported that historically TSA has not tracked statistics regarding whether VIPR deployments were driven by specific intelligence, versus being random, broadly risk-based, or special event driven. However, program officials stated that there have been few instances when TSA deployed VIPR teams to mass transit and passenger rail on the basis of specific threat information. In February 2009, TSA officials reported that they had amended the VIPR database to track the reasons for future VIPR deployments.

⁵⁶ TSA's *Concept of Operations for the Effective Employment of VIPR teams in Mass Transit and Passenger Rail* lays out guidelines for ten core components that are the foundation for effectively collaborating on VIPR programs, including: (1) coordination; (2) mission focus; (3) active deterrence; (4) planning; (5) force composition; (6) consistency; (7) training; (8) communications; (9) authority; and (10) continuous improvement.

⁵⁷ Department of Homeland Security Inspector General, *TSA's Administration and Coordination of Mass Transit Security Programs* (June 12, 2008).

review of TSA after-action reports for 104 VIPR operations TSA conducted from November 2007 through July 2008 on mass transit and passenger rail systems—a nine month period after TSA issued the CONOPS guidance—identified insufficient interoperable radio communications as a key challenge faced during many VIPR operations.

According to the after-action reports, TSA's key challenge has been ensuring that its VIPR teams have reliable interoperable radio communications—both among TSA personnel and with local law enforcement. According to the CONOPS, ensuring interoperable radio communications between VIPR team members and local law enforcement is essential to the safe and effective execution of VIPR programs, including ensuring their ability to communicate information on potential threats encountered during operations. However, in almost half of the after-action reports we reviewed (49 of 104), VIPR participants reported that a lack of reliable communications equipment had hindered their ability to conduct real-time communications with local law enforcement. This challenge has existed since TSA expanded the VIPR program into mass transit and passenger rail systems, where cell phone or other communications systems that previously worked in airports did not effectively operate in a transit environment. In many cases, TSA field personnel reported requests for new interoperable radio systems, but had not had those requests fulfilled by TSA headquarters. These reports indicated the need for a more comprehensive solution in which TSA procures communications systems capable of real time interoperability with security partners in mass transit and passenger rail systems.

TSA managers of the VIPR program acknowledged the challenges that the VIPR program had experienced since it expanded into mass transit and passenger rail systems and stated that the agency was taking actions to address them. Examples include:

- **Communications Improvements:** TSA reported deploying additional communications equipment to field locations and working with DHS S&T to test new technologies for enhancing communications capability and interoperability in a mass transit or passenger rail environment.
- **Coordination and Awareness:** TSA reported that it developed and made available to mass transit and passenger rail systems a brochure with information on scheduling and deploying VIPR operations, including a description of the different options available for systems in utilizing VIPR teams and the planning and operational roles and

responsibilities of participating TSA personnel.⁵⁸ Further, to improve nationwide coordination of VIPR operations, TSA established a coordination center dedicated solely to VIPR operations and has established dedicated mobile VIPR teams in 10 cities. TSA has reported that it plans to expand the number of these teams nationwide by 2010.

- **Training TSA Personnel:** TSA reported in February 2009 that the agency had begun requiring VIPR team personnel to participate in system orientation and safety training from mass transit and passenger rail systems where they deploy in order to familiarize VIPR team members with both the transit agency's physical structure and operating procedures. TSA also reported offering additional training on surface-based law enforcement tactics and legal authorities.

Because TSA plans to further expand the VIPR program in 2009, effectively implementing these actions should better ensure that TSA uses its limited security resources to maximize the security benefit of VIPR operations in mass transit and passenger rail.

TSA Established a Program to Expand Security Training for Mass Transit and Passenger Rail Employees, but Opportunities Exist to Strengthen It

In February 2007, TSA established a training program to assist mass transit and passenger rail agencies in expanding security training for their frontline transit employees. However, opportunities exist for TSA to strengthen its process for ensuring consistency in the performance of non-federal training vendors that mass transit and passenger rail agencies use to obtain training through the program. After TSA's initial BASE reviews revealed wide variations in the extent of training that transit agencies were providing to their employees, including limited recurrent training, TSA established a Mass Transit Security Training program to provide curriculum guidelines for basic and follow-on security training areas—training programs and courses largely developed and funded by FTA. It also specified areas in which particular categories of employees should receive recurrent training as well as a matrix tool to enable transit agencies to determine the costs and timelines for implementing the training. To support delivery of the training courses, TSA aligned the program with the DHS Transit Security Grant Program. The Transit Security Grant Program has made transit agency grant funding for security

⁵⁸ In addition, TSA reported it was developing a VIPR tool kit concept to be distributed to mass transit systems and TSA field staff, which will contain an educational DVD explaining the potential security value of VIPR operations. The tool kit is projected for completion by June 2009, with initial distribution at the mid-year Transit Safety and Security Roundtable.

training a top priority and 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.⁵⁹

While TSA has reported that the Mass Transit Security Training Program is providing opportunities for mass transit and passenger rail systems to expand security training to their employees, senior officials from FTA's Safety and Security Office expressed concern that TSA had not established the necessary criteria to effectively manage the program. According to TSA's Mass Transit Security Training Program guidance, 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.⁶⁰ As a result, TSA assumed new responsibility for evaluating whether these security training vendors met the performance standards of federally sponsored training providers and whether they could be used by transit agencies for training under the Transit Security Grant Program.⁶¹ However, opportunities exist for TSA to strengthen its process for making this evaluation. According to TSA, transit agency requests to use non-federally funded or sponsored training vendors under the Transit Security Grant Program are reviewed by TSA's mass transit training specialist and by FEMA's Grants Program Directorate for approval. This review includes an analysis of course documentation, such as a description of the course syllabus, cost estimate, and justification for why the course was the preferred solution. However, both FTA and TSA officials acknowledged that additional criteria are needed for TSA to properly evaluate the selection of the training vendors. As the lead federal agency for developing and implementing mass transit employee safety training programs since 1971, FTA is in the process of

⁵⁹ According to TSA's program guidance for the Mass Transit Security Training Program, only underground or underwater tunnel infrastructure rank as high as security training among its security priorities.

⁶⁰ According to the TSA guidance, federally sponsored training providers are FTA-funded training providers including the National Transit Institute (NTI), the Transportation Safety Institute (TSI), and Johns Hopkins University (JHU).

⁶¹ According to the guidance, DHS must review transit agency applications for non-federally sponsored or funded training vendors 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 providers.

issuing guidance that could be relevant to TSA's evaluation of training vendors. According to FTA's 2009 Training Curriculum Development Guidelines, scheduled for release in 2009, criteria for evaluating the quality of training services should include, among other things, a review of the credentials of the instructors who would deliver the training course, the training vendor's experience in providing the security course, and any performance evaluations or feedback obtained from organizations and students who previously received training from the vendor.⁶² Additionally, as we reported in March 2004, agencies should try to develop clear criteria when determining whether to contract with vendors for training.⁶³ We identified factors that agencies should consider include the prior experience, capability, and stability of the vendors offering the training.

Since implementing the Mass Transit Security Training Program in 2007, TSA reported that about 50 mass transit and passenger rail systems had applied for Transit Security Grant Program funding for employee security training, including one agency that applied to use training vendors that are not federally funded or sponsored. However, more applications for this option are expected as additional grant funding for training becomes available. TSA and FTA officials both noted their preference for transit agencies to use federally-sponsored training providers and expressed concerns that increased demands on the providers may make scheduling training with federally funded or sponsored providers more difficult. Enhancing criteria for evaluating the quality of training services could strengthen DHS's ability to ensure that the grant money DHS is awarding to mass transit and passenger rail agencies is consistently funding sound and valid security training programs for these employees. In October 2005, we reported that collaborating agencies can identify opportunities to leverage each other's resources, thus obtaining additional benefits that would not be available by working separately.⁶⁴ By coordinating the enhancement of these criteria with other agencies conducting similar efforts, such as FTA, TSA could also leverage the expertise of other agencies to better ensure its efforts result in sound criteria.

⁶² U.S. Department of Transportation, Federal Transit Administration, *Curriculum Development Guidelines: Final Draft* (2009).

⁶³ GAO, *A Guide For Assessing Strategic Training and Development Efforts*, [GAO-04-546G](#) (Washington D.C: March 2004).

⁶⁴ GAO, *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, [GAO-06-15](#) (Washington D.C: Oct. 21, 2005).

TSA Reported Implementing Some 9/11 Commission Act Provisions for Mass Transit and Passenger Rail Security, but Implementing New Regulations May Pose Challenges for TSA and Industry Stakeholders

In March 2009, TSA reported that it had implemented some of the 9/11 Commission Act's provisions related to mass transit and passenger rail security. While most mass transit and passenger rail industry security actions have been voluntary to date, the 9/11 Commission Act sets forth mandatory requirements for federal and industry stakeholders, and implementing those requirements may pose challenges for TSA and industry stakeholders, particularly for TSA's Surface Transportation Security Inspection Program. TSA has more than doubled the size of its Surface Transportation Security Inspection Program over the past year, but has not completed a workforce plan to address current and future program needs, and surface inspectors have reported concerns with organizational changes that TSA has made to the program that may affect implementation of new responsibilities. Additionally, officials from the mass transit and passenger rail industry have reported concerns with the cost and feasibility of implementing pending 9/11 Commission Act regulations.

TSA Reported Implementing Some Provisions of the 9/11 Commission Act for Mass Transit and Passenger Rail Security

The 9/11 Commission Act, enacted in August 2007, contains many provisions that task TSA with implementing various actions related to surface transportation, including mass transit and passenger rail security. Among other things, these provisions identify mandates for developing and issuing reports on TSA's strategy for securing public transportation, conducting and updating security assessments of mass transit systems, and establishing a program for conducting security exercises for transit and rail agencies. In March 2009, TSA reported that it had satisfied some provisions of the 9/11 Commission Act pertaining to mass transit and passenger rail, including some through actions that had been taken prior to the enactment of the 9/11 Commission Act. For example, TSA reported that it had issued a report on the transportation security enforcement process and that its Mass Transit Modal Annex satisfied the requirement to develop a strategy for securing public transportation. However, TSA also reported that it had not yet implemented a number of other 9/11 Commission Act provisions, including several requiring TSA to issue regulations that would place new requirements on the mass transit and passenger rail industry.

The 9/11 Commission Act requires TSA to develop and issue several different regulations for mass transit and passenger rail, including regulations for employee security training programs and requiring high-risk rail carriers to develop and implement security plans. TSA reported that it was in the process of developing these regulations and that for some required regulations it had sought feedback from the transit industry

as it developed new regulations. However, as of March 2009, TSA had missed several legislative deadlines for issuing the required mass transit and passenger rail regulations, and in some cases had not established time frames for when it would ultimately do so. For example, TSA was required to issue interim regulations outlining requirements for a mass transit employee security training program by November 2007, with final regulations due by August 2008. TSA was also required to issue regulations by August 2008 requiring high-risk rail carriers to develop and implement security plans. However, TSA did not meet these deadlines. TSA reported that deadlines in the act for developing and issuing new regulations have been difficult to meet because of different factors, including the comprehensive scope of the requirements, the need to coordinate them with various entities, and a lack of resources for completing certain tasks. See table 6 below for a list of key selected 9/11 Commission Act mass transit and passenger rail provisions mandating actions by TSA, along with TSA's reported status in doing so, as of March 2009.

Table 6: Key Selected Provisions of the 9/11 Commission Act for Mass Transit and Passenger Rail Security and TSA's Reported Implementation Status, as of March 2009

Section	Requirement	TSA reported status
Strategies		
§ 1404	Develop and implement the National Strategy for Public Transportation Security.	TSA reported that the Mass Transit Modal Annex to the Transportation System -Sector Specific Plan meets this requirement.
§ 1511	Establish a task force to complete (by Feb. 2008) a risk assessment of a terrorist attack on railroad carriers, and based on the assessment, develop and implement the National Strategy for Railroad Transportation Security.	TSA reported that the task force has been established and that the National Strategy for Railroad Transportation Security is under development. For passenger rail, TSA reported that the Mass Transit Modal Annex to the Transportation System -Sector Specific Plan meets the requirement to develop and implement a security strategy.
Vulnerability assessments and security plans		
§ 1405	Review and update FTA security assessments of high-risk public transportation agencies, require high-risk public transportation agencies to develop security plans and review, amend as necessary, and approve the security plans.	TSA reported that FTA security assessments were provided to TSA and that TSA used the BASE program to update the assessments. TSA stated that it will use the BASE results in developing regulations implementing this requirement. TSA reported that a regulatory project has been initiated.
§ 1405(b)	Conduct security assessments to determine the specific needs of local bus-only transportation systems.	TSA reported that the assessments have been completed and that information is being prepared for use by the transportation system operators.

Section	Requirement	TSA reported status
§ 1512	Issue regulations (by Aug. 2008) that require each railroad carrier, including passenger rail carriers, determined to be high-risk to conduct a vulnerability assessment and to prepare, submit for approval, and implement a security plan.	TSA reported that a regulatory project has been initiated.
Exercise programs		
§ 1407, § 1516	Establish a program for conducting security exercises for public transportation agencies and for railroad carriers. Establish a program for conducting security exercises for railroad carriers, including passenger rail carriers.	TSA reported that its Intermodal Security Training and Exercise Program meets this requirement. The agency further reported a multi-phased, multi-jurisdictional pilot of this exercise program was held in the National Capitol Region from January through June 2008, northern New Jersey in September 2008, and Los Angeles from February to June 2009.
Training programs		
§ 1408, § 1517	Issue interim (by Nov. 2007) and final regulations (by Aug. 2008) for a public transportation security training program and issue regulations (by Feb. 2008) for a security training program for frontline railroad, including passenger railroad, employees.	TSA reported that a consolidated regulatory project including public transportation, railroad, and over-the-road bus has been initiated. TSA reported that it anticipates issuing a Notice of Proposed Rulemaking in late calendar year 2009 or early calendar year 2010.
Background checks		
§ 1411, § 1520	Complete a name-based security background check for all public transportation frontline employees and frontline railroad employees.	TSA reported that it has begun to develop a project plan for a rulemaking needed to satisfy this requirement, but that significant funding and time will be required to meet this requirement.

Source: GAO analysis of TSA data.

TSA reported that it tracks the implementation status of mass transit and passenger rail security provisions of the 9/11 Commission Act on a monthly basis as part of a DHS-managed working group and was identifying processes needed to implement the provisions. TSA provided us with progress reports for completing these provisions which, in certain cases, identified challenges it faced in doing so, including a lack of resources. But the reports did not include a plan for addressing these challenges or milestones for implementing several 9/11 Act Commission provisions, as called for by project management best practices.⁶⁵ TSA officials reported that before they could move forward on the 9/11

⁶⁵ Project Management Institute, *The Standard for Program Management* (Newton Square, PA, 2006).

Commission Act requirements, they needed to allow the new administration time to review TSA's efforts to date. However, until TSA develops a plan with milestones, it will be difficult to provide reasonable assurance that the provisions of the act are being developed and that a strategy is in place for overcoming identified challenges.

While Industry Security Actions Have Largely Been Voluntary, New 9/11 Commission Act Requirements Outline a Mandatory Approach and Pose Challenges for TSA's Inspectors

While the majority of industry actions to secure mass transit and passenger rail have been taken on a voluntary basis, the pending 9/11 Commission Act regulations outline a new approach that sets forth mandatory requirements, the implementation of which may create challenges for TSA and industry stakeholders. With the exception of the 2004 passenger rail security directives, TSA had not, until recently, imposed security requirements on the mass transit and passenger rail industry. Instead TSA took a collaborative approach in encouraging passenger rail systems to voluntarily participate and address security gaps through its BASE review program.⁶⁶ With TSA's pending issuance of regulations required by the 9/11 Commission Act, TSA will fundamentally shift this approach, and establish a new regulatory regime for mass transit and passenger rail security.

Once TSA issues the pending regulations for mass transit and passenger rail security, TSA's Surface Transportation Security Inspection Program would have responsibility for enforcing industry compliance—further expanding and evolving the roles and responsibilities these inspectors have for mass transit and passenger rail, in addition to their responsibilities for other surface modes, such as freight rail, highway, and motor carrier security. TSA officials have raised concerns about their ability to meet the growing inspection requirements for mass transit and passenger rail and other surface modes that will be incurred by the new regulations required by the 9/11 Commission Act, particularly because TSA's Surface Transportation Security Inspection Program is already challenged to meet its existing workload. For example, 10 of 11 Surface Transportation Security Inspection Program field office supervisors—Assistant Federal Security Directors for Surface Transportation (AFSD-S)—whom we interviewed reported that while they were meeting their primary inspection responsibilities for mass transit and other surface modes, resource constraints were routinely leading them to delay

⁶⁶ TSA reported that the pending regulations required by the 9/11 Commission Act requiring transit agencies to issue security plans would supersede the existing security directives.

secondary activities, such as conducting stakeholder outreach with mass transit and passenger rail agencies.⁶⁷ These field office supervisors attributed their resource constraints to a significantly expanded Surface Transportation Security Inspection Program workload from fiscal year 2006 through 2008 without a corresponding increase in its workforce. During this time, TSA expanded the responsibilities of the surface transportation security inspectors to include additional surface transportation modes, including conducting various voluntary security inspections for mass transit bus and freight rail, and participating in VIPR operations.⁶⁸

TSA's Surface Transportation Security Inspection Program is at risk of being unable to meet its expanding responsibilities if it does not plan for how to meet them. TSA reported that the agency had been appropriated funding to hire an additional 125 surface inspectors that would more than double its surface inspector workforce—including 75 in fiscal year 2008 and 50 more in fiscal year 2009—and planned to complete their hiring, training, and deployment by the end of fiscal year 2009.⁶⁹ TSA reported plans to largely dedicate its newly hired surface inspectors to conducting VIPR activities, assessing security activities on surface modes, and monitoring newly issued freight rail security rules, such as ensuring a secure chain of custody for certain hazardous materials.⁷⁰ However, as reported by the DHS Inspector General, beyond supporting current activities, the additional manpower TSA plans to put into its Surface

⁶⁷ We interviewed 11 of 12 AFSD-S that, as of February 2009, TSA has deployed nationwide to lead area inspection offices. At the time, two AFSD-S shared duties in the New York field office and were interviewed together.

⁶⁸ TSA's fiscal year 2009 Regulatory Activities Plan for Transportation Surface Inspectors requires surface inspectors to split their assessment workload between mass transit and passenger rail and freight, with a minimum of about 60 percent of their time dedicated to freight and 40 percent to mass transit and passenger rail.

⁶⁹ From fiscal year 2005 through fiscal year 2007, the Surface Transportation Security Inspection Program was authorized at 100 full-time employees and in June 2008 reported a staffing level of 93 positions. The 9/11 Commission Act authorized DHS to increase its number of surface transportation security inspectors for fiscal years 2008 through 2011 to a maximum of 200 positions. In February 2009, TSA reported that it had completed hiring for 58 of the 75 surface inspector positions that had been appropriated in fiscal year 2008, but had not filled the remaining positions because of contractor hiring challenges.

⁷⁰ On November 26, 2008, TSA issued a final rule for freight rail and passenger rail that establishes security requirements on freight and passenger rail carriers, including designating a rail security coordinator and reporting significant security concerns, and codifies TSA's authority to conduct security inspections of passenger rail agency property.

Transportation Security Inspection Program may provide only limited relief.⁷¹ As a result, even with these additional resources, TSA's surface inspectors may face challenges in fulfilling their responsibilities.

GAO guidance on strategic human capital management reinforces that high performing organizations conduct workforce planning and analysis to identify and prepare for current and future workforce needs.⁷² Accordingly, a workforce plan that includes an analysis of a program's workforce needs can help to ensure that the program has the right amount of resources to achieve program goals, allowing program managers to spotlight areas for attention before problems develop. In February 2009, we reported that TSA did not have a human capital or other workforce plan for its Transportation Security Inspection Program, but the agency had plans to conduct a staffing study to identify the optimal workforce size to address its current and future program needs.⁷³ TSA reported that it had hired a contractor to conduct a full workforce analysis of its security inspectors, including both its aviation and surface inspectors, to determine the number needed to fulfill expanded roles and responsibilities and ensure effective deployment. TSA reported that it had initiated the study in January 2009 to be completed in late fiscal year 2009.⁷⁴ This study, if completed, should provide TSA with a more reasonable basis for determining the surface inspector workforce needed to achieve its current and future workload needs in light of the new requirements of the 9/11 Commission Act.⁷⁵

⁷¹ The DHS Inspector General has issued two recent reports on TSA's mass transit security programs. These include Department of Homeland Security Office of the Inspector General, *TSA's Administration and Coordination of Mass Transit Security Programs*, OIG-08-66 (June 12, 2008) and Department of Homeland Security Office of the Inspector General, *Effectiveness of TSA's Surface Transportation Security Inspector*, OIG-09-24, (Feb. 5, 2009).

⁷² GAO, *Key Principles for Effective Strategic Workforce Planning*, [GAO-04-39](#) (Washington D.C.: Dec. 11, 2003).

⁷³ GAO, *Aviation Security: Aviation Security: Status of Transportation Security Inspector Workforce*. [GAO-09-123R](#) (Washington, D.C.: Feb. 6, 2009).

⁷⁴ In fiscal year 2008, TSA reported that it had deployed a total of 1224 inspectors into the aviation and surface modes, 1131 of whom were aviation inspectors.

⁷⁵ TSA's Surface Transportation Security Inspection Program strategic plan for fiscal year 2008 notes that the program expects to expand its roles and responsibilities to enforce compliance with future mass transit and passenger rail regulations and notes challenges in meeting its current responsibilities because of resource limitations.

Stakeholders Have Raised Concerns Regarding Changes to TSA's Surface Transportation Security Inspection Program Field Office Command Structure

Surface inspectors have raised concerns about recent organizational changes that TSA has made to the Surface Transportation Security Inspection Program that may affect the implementation of its expanded roles and responsibilities. These concerns were reported by Surface Transportation Security Inspection Program field officials we interviewed, two recent DHS-IG reports, and an internal TSA report prepared by several Surface Transportation Security Inspection Program field officials.⁷⁶ Specifically, in April 2008, TSA announced plans to expand the number of Surface Transportation Security Inspection field offices nationwide, from 22 to 54. Under a re-organized reporting structure, TSA placed 31 of the 32 new field offices under the command of Federal Security Directors and Assistant Federal Security Directors for Inspections—aviation-focused positions that historically have not had an active role in conducting mass transit, passenger rail, or other surface transportation inspection duties. TSA's Surface Transportation Security Inspection Program headquarters officials continue to set strategy and annual goals, while in most field offices the surface inspectors report to the Federal Security Directors and Assistant Federal Security Directors for Inspections, who have day-to-day management lead and hiring responsibilities for surface inspectors. Reported field official concerns include:

- **Balancing aviation and surface transportation priorities:** A January 2008 report that 6 of 12 of TSA's Assistant Federal Security Directors for Surface submitted to TSA headquarters cited concerns that placing the Surface Transportation Security Inspection program under the Federal Security Directors had resulted in the surface transportation mission being diluted by TSA's aviation mission. The report also stated that the current reporting line of surface inspectors is less efficient and may create confusion among surface inspectors, because Federal Security Directors' priorities and needs differ from those of the surface program.
- **Establishing and maintaining credibility with industry stakeholders:** Eight of the 11 Assistant Federal Security Directors for Surface we interviewed reported concerns that Federal Security Directors were not sufficiently focused on mass transit and passenger rail and the different challenges that surface inspectors face in overseeing the industry's voluntary participation in non-regulatory security assessment activities. For example, one Assistant Federal Security Director for Surface commented that Federal Security

⁷⁶ OIG-09-24 and OIG-08-66.

Directors had tasked aviation security officers to participate in surface assessments and that doing so had caused some frustration among transit agency officials because of their lack of knowledge about the transit environment. A June 2008 DHS-IG report also noted surface inspectors' concerns that Federal Security Directors were hiring surface inspectors who had no prior surface transportation experience, and that in some cases, Assistant Federal Security Directors reported that they were not included in hiring decisions.

TSA disagreed with the DHS-IG and Assistant Federal Security Directors reports' findings that the present Surface Transportation Security Inspection Program field office command structure had inhibited the program's effectiveness. For example, TSA did not concur with the DHS-IG's recommendation that TSA place the Surface Transportation Security Inspection Program under the direct authority of a TSA headquarters official responsible for surface transportation, rather than under the Federal Security Directors. TSA reported that they had selected their current command structure because Federal Security Directors were best equipped to make full use of the security network in their geographical location because they frequently interacted with state and local law enforcement and mass transit operators, and were aware of vulnerabilities in these systems.

Transit Industry Stakeholders Expressed Concern about the Cost and Feasibility of Implementing Pending Regulatory Requirements

While TSA has not yet issued the new 9/11 Commission Act regulations for mass transit and passenger rail, 12 of 30 mass transit and passenger rail agencies we interviewed raised potential implementation concerns associated with one expected regulatory requirement regarding training for mass transit and passenger rail employees. Among other comments, mass transit and passenger rail agency officials reported that unless these new regulations were accompanied by funding to address implementation costs, they would be challenged to comply since mass transit agencies face tight budgetary constraints. For example, one transit agency official reported in feedback to TSA that an agency with 5,000 employees would incur labor costs of \$1.5 million to have its employees participate in an 8-hour training program. Another transit agency official reported that it would be an achievement to get 30 to 40 percent of frontline employees through training in a year due, in part, to the costly overtime for backfilling those employees' positions while they are in training. Additionally, these 12 agencies also reported concerns about the logistical feasibility of implementing the training requirement. For instance, under the act, mass transit and passenger rail agencies would be required to complete security training for all of their frontline employees within one year of DHS's

approving the transit agency's training program. However, several mass transit and passenger rail agencies reported having thousands of employees and said it would be difficult to schedule training for all employees within one year without disrupting operations because they did not have the staff needed to backfill the positions of the employees undergoing training.

Conclusions

As terrorist attacks on mass transit and passenger rail systems overseas have made clear, even with a variety of security precautions in place, mass transit and passenger rail systems that move high volumes of passengers on a daily basis remain vulnerable to attack. Since 2004, TSA has introduced a variety of initiatives aimed at enhancing the security of the nation's mass transit and passenger rail systems, including conducting security assessments, implementing new security programs, and implementing some provisions of the 9/11 Commission Act. However, given the importance of the mass transit and passenger rail systems, the inherent vulnerabilities that could be exploited by terrorist threats, and the broadening requirements that will result in a shift to a regulatory approach, addressing management and coordination challenges should help ensure that current and future actions effectively improve the security of these systems. TSA has taken key steps to help secure the nation's mass transit and passenger rail systems; however, additional actions to more effectively target resources would strengthen TSA's security approach. To ensure that TSA's efforts best prioritize and address risks, TSA should conduct a risk assessment for the mass transit and passenger rail systems that combines the results of threat, vulnerability, and consequence assessments. Until the overall risk to the entire system is identified through such an assessment, TSA cannot best determine how and where to target its limited resources to achieve the greatest security gains. TSA's 2007 Mass Transit Modal Annex represents a positive step toward documenting TSA's strategy for securing the mass transit and passenger rail systems, but further refinements to the strategy documented in future updates to the Modal Annex would help ensure that it provides all stakeholders with a clear and measurable path forward. For example, including relevant performance metrics will allow stakeholders to better evaluate their progress in achieving the strategy's vision. In addition, incorporating information on what the strategy will cost, to the extent possible, would help implementing parties allocate budgets according to priorities and constraints, and would help stakeholders shift such investments and resources as appropriate.

Federal and industry efforts to work together in securing mass transit and passenger rail in the absence of any significant federal security regulations have been commendable. In particular, TSA's BASE reviews have been a positive step as they enhanced the awareness of security vulnerabilities at mass transit and passenger rail agencies throughout the country, while strengthening relationships among transit stakeholders. Notwithstanding TSA's progress, TSA's efforts remain largely in the early stages and opportunities exist for TSA to strengthen the implementation of some of its security programs. Expanding its outreach with mass transit and passenger rail officials will be particularly important for TSA in gathering security technology information and disseminating it to the systems and enabling officials to identify and deploy new security technologies to better secure their systems. In addition, with HSIN, TSA already has a venue in place for expanding the dissemination process and should explore the feasibility of populating this site with better and more relevant technology information to help meet the needs of mass transit and passenger rail agencies regarding information on available security technology. Such action should help ensure that limited resources are not used to duplicate research and testing efforts. Finally, by providing guidance and funding to cover mass transit and passenger rail agency costs for providing employee security training, TSA has taken steps to reduce a key vulnerability it identified during its BASE reviews. However, with the anticipated increase in demand for employee security training, it is important that TSA have an effective evaluation process in place to ensure it is consistently funding sound and valid training programs for mass transit and passenger rail agencies seeking funding to pay for non-federal training providers.

Finally, a significant transition lies ahead. While TSA reports making progress in implementing the provisions of the 9/11 Commission Act, the agency has fallen behind in issuing required mass-transit and passenger-rail security regulations. The implementation of these regulations will be a fundamental shift in approach for TSA as it assumes more of a regulatory role in securing mass transit and passenger rail. This shift—combined with an expanding Surface Transportation Security Inspector workforce that has more than doubled in size in the past year and shifting deployment and field reporting structures—will challenge TSA to manage its new responsibilities. However, this transition will be important for both TSA and industry stakeholders to manage successfully to ensure that new requirements are met and that TSA and stakeholders continue to work together to secure mass transit and passenger rail. One approach that could help DHS manage these many changes is to develop a schedule with milestones for implementing the remaining 9/11 Commission Act

requirements pertaining to mass transit and passenger rail. Without such a plan, it will be difficult for TSA to provide reasonable assurance that the provisions of the act are being implemented and that a strategy is in place for overcoming identified challenges. We recognize the inherent challenges to securing these systems given the continuing terrorist threat, openness of the system, and difficulties posed by attempting to secure and patrol numerous points of entry. However, given the criticality of mass transit and passenger rail systems to our way of life and the economy, and the inherent risks to them, TSA should continue to strive to strengthen its security efforts for the systems.

Recommendations for Executive Action

To help ensure that the Transportation Security Administration is successfully prioritizing resources and collaborating with federal and industry stakeholders in implementing actions to secure the mass transit and passenger rail systems from acts of terrorism, and that its strategy is consistent with the characteristics of a successful national strategy, we are making six recommendations to the Assistant Secretary for the Transportation Security Administration:

- To help ensure that the federal strategy to secure the mass transit and passenger rail systems considers assessment information within the context of risk, TSA, as the sector-specific agency for mass transit and passenger rail, should conduct a risk assessment that integrates all three elements of risk—threat, vulnerability, and consequence. As part of this assessment, TSA should, to the extent feasible, fully leverage existing assessment information from its own sources as well as those provided by other federal and industry stakeholders, as appropriate, and use this information to inform its security strategy.
- To better achieve the security strategy laid out in its Mass Transit Modal Annex—TSA’s security strategy for the mass transit and passenger rail systems—TSA should, to the extent feasible, incorporate into future updates of the Modal Annex the characteristics of a successful national strategy and the elements outlined in Executive Order 13416, including:
 - measuring the agency’s and industry’s performance in achieving the goals of preventing and deterring acts of terrorism and enhancing the resiliency of mass transit and passenger rail systems and

-
- incorporating information on what the strategy will cost along with the specifying the sources and types of resources and investments needed, and identifying where those resources and investments should be targeted.
 - To help ensure that DHS security technology research and development efforts reflect the security technology needs of the nation's mass transit and passenger rail systems, TSA should expand its outreach to the mass transit and passenger rail industry in the planning and selection of related security technology research and development projects.
 - To meet the needs of mass transit and passenger rail agencies regarding information on available security technologies, TSA should explore the feasibility of expanding the security technology product information on the Public Transit Portal of the Homeland Security Information Network, and consider including information such as product performance in a rail or bus venue, cost, maintenance needs, and other information to support mass transit and passenger rail agencies purchasing and deploying new security technologies.
 - 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 criteria could be used by transit agencies for training under the transit security grant program. As part of this effort, TSA should consider coordinating with other federal agencies that have developed criteria for similar programs, such as the Federal Transit Administration.
 - To better ensure DHS's ability to satisfy the provisions of the 9/11 Commission Act related to mass transit and passenger rail, DHS should develop a plan with milestones for implementing provisions of the 9/11 Commission Act related to mass transit and passenger rail security.

Agency Comments

We provided a draft of this report to DOT, Amtrak, and DHS for review and comment. DOT did not provide comments. Amtrak provided written comments on June 16, 2009. In its letter, Amtrak provided additional information on security actions they were taking, noted collaboration with federal agencies, and expressed some concern about the cumbersome nature and cost share requirements of the Transit Security Grant Program. Amtrak's comments are presented in appendix VII. DHS provided written

comments on June 17, 2009, which are presented in appendix VIII. In commenting on the report, DHS stated that it concurred with all six recommendations and identified actions planned or under way to implement them.

In comments related to our first recommendation, that DHS conduct a risk assessment that integrates all three elements of risk, DHS stated that it recognized the importance of conducting risk assessments to inform agency priorities, security enhancement programs, and resource allocations. It also reported that in addition to the various assessments already completed and the BASE reviews conducted on a continuous cycle, an assessment pilot program is planned for later in 2009. Under this pilot, TSA will evaluate the effectiveness of and provide lessons learned from its new risk assessment tool for mass transit and passenger rail to enhance the tool's capability prior to its implementation. In comments related to our second recommendation that DHS incorporate in future updates of the Modal Annex the characteristics of a successful national strategy and the elements outlined in Executive Order 13416, DHS reported that it planned to revise its Mass Transit Modal Annex and incorporate these characteristics and elements to improve its ability to measure agency and industry progress toward achieving mass transit and passenger rail security performance goals. In response to our third recommendation that TSA expand its outreach to the mass transit and passenger rail industry in the planning and selection of related security technology research and development projects, DHS reported on several planned coordination efforts including its intent to coordinate the Modal Annex update with mass transit and passenger rail stakeholders, and work to ensure that stakeholders have ample opportunities to provide input on security technology development and testing priorities. With regard to our fourth recommendation that TSA explore the feasibility of expanding the security technology product information on the Public Transit Portal of the Homeland Security Information Network, DHS reported that it expects to expand both the scope and quality of security technology information provided to stakeholders through the Public Transportation Information Sharing and Analysis Center—which has a principal objective of aligning and integrating analytical and information sharing activities with relevant federal processes to enhance the information-sharing environment for the mass transit and passenger rail community. In comments related to our fifth recommendation that TSA consider enhancing its criteria for evaluating security training vendors under the Transit Security Grant Program and consider coordinating with other federal agencies that have developed such criteria, DHS stated that TSA will work with FTA through an existing joint working group to develop criteria for reviewing new

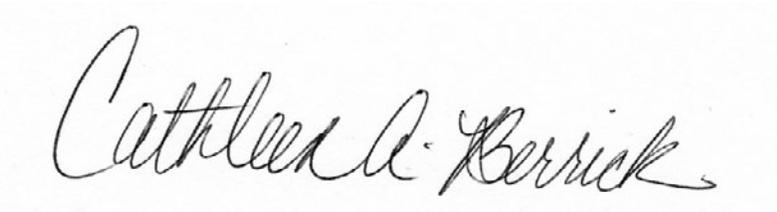
vendor-provided training courses. Lastly, with regard to our sixth recommendation that DHS develop a plan with milestones for implementing provisions of the 9/11 Commission Act related to mass transit and passenger rail security, DHS reported that TSA will produce a plan that identifies necessary actions and sets milestones to evaluate its effectiveness in meeting statutory requirements associated with the 9/11 Commission Act.

DHS and Amtrak also provided us with technical comments, which we considered and incorporated into the report where appropriate.

As agreed with your office, unless you publicly announce the contents of this report, we plan no further distribution for 30 days from the report date. At that time, we will send copies of this report to the Secretary of Homeland Security, the Secretary of Transportation, Amtrak, interested congressional committees, and other interested parties. The report will also be available at no charge on the GAO Web site at <http://www.gao.gov>.

If you or your staff have any questions concerning this report, or wish to discuss these matters further, please contact me at (202) 512-3404 or berrickc@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix IX.

Sincerely yours,

A handwritten signature in black ink that reads "Cathleen A. Berrick". The signature is written in a cursive style with a large initial 'C' and a long, sweeping tail on the 'k'.

Cathleen A. Berrick
Managing Director, Homeland Security and Justice Issues

Appendix I: Objectives, Scope, and Methodology

The objectives of this report were to: (1) determine the extent that federal and industry stakeholders assessed or supported assessments of the security risks to mass transit and passenger rail since 2004, and how, if at all, TSA used risk assessment information to inform and update its security strategy; (2) describe key actions, if any, that federal and industry stakeholders implemented or initiated, since 2004, to strengthen the security of mass transit and passenger rail systems, the extent to which federal actions were consistent with TSA's security strategy, and what challenges, if any, TSA faces in implementing these actions; and (3) describe TSA's reported status in implementing provisions of the Implementing Recommendations of the 9/11 Commission Act of 2007 related to mass transit and passenger rail security, and discuss challenges, if any, TSA and the mass transit and passenger rail industry face in implementing the actions required by the act.

To determine the extent that federal and industry stakeholders have assessed or supported assessments of the security risks to mass transit and passenger rail since 2004, and how, if at all, TSA has used risk assessment information to inform and update its security strategy, we obtained and analyzed various reports that address some or all elements of security risk (threat, vulnerability, and consequence) from DHS component agencies, including TSA, the DHS Office of Infrastructure Protection within the National Protection and Programs Directorate (NPPD), and the Homeland Infrastructure Threat Reporting and Analysis Center (HITRAC). We also reviewed information on risk-related assessments conducted by federal agencies, including mass transit and passenger rail security vulnerability assessments conducted by DOT's Federal Transit Administration (FTA), and a variety of federally developed security risk assessment tools for the mass transit and passenger rail industry.

Additionally, we reviewed TSA's Baseline Assessment for Security Enhancement (BASE) review checklist and fiscal year 2007 BASE report of the results of BASE reviews that TSA conducted at 44 of the top 50 largest mass transit and passenger rail agencies—by ridership—as a measure of TSA's efforts to gather vulnerability information. We gathered information on TSA's consequence assessments through interviews with Transportation Sector Network Management (TSNM) officials. We also interviewed TSNM officials in order to assess how risk assessments were informing TSA's security strategy for mass transit and passenger rail and

then compared TSA's actions to GAO and DHS reports on risk assessment.¹ Because of the scope of our work, we relied on TSA to identify its assessment activities but did not assess the extent to which its assessment activities meet the National Infrastructure Protection Plan criteria for threat, vulnerability, and consequence assessments.

To further assess risk assessment efforts, we interviewed federal officials from DHS's HIRAC, TSA's Office of Intelligence, TSA's Surface Transportation Security Inspection Program, and, at DOT, FTA's Office of Safety and Security to understand what additional assessment information or assistance on risk assessments was available to either TSA or the transit agencies. Further, we interviewed security officials from Amtrak and 30 mass transit and passenger rail agencies across the nation. This sample allowed us to meet with agencies of varying sizes and types to determine their perspectives on federal and mass transit and passenger rail industry risk assessment efforts to date (see objective 2 for how these agencies and cities were selected).

Additionally, we reviewed TSA's strategic planning document—the Mass Transit Modal Annex to the Transportation System - Sector Specific Plan (TS-SSP) issued in May 2007—and identified federal guidelines for developing a risk-based security strategy. Specifically, to determine the extent to which TSA's strategy conformed to requirements and best practices, we reviewed relevant statutory requirements of the Government Performance and Results Act of 1993 (GPRA) that included general requirements that are applicable in the establishment of government strategies and programs, and the Implementing Recommendations of the 9/11 Commission Act of 2007, which included requirements for establishing a security strategy. For example, we reviewed existing Executive Directives, including Homeland Security Presidential Directives 1, 7, and 8, and Executive Order 13416: *Strengthening Surface Transportation Security* to determine the extent to which TSA's Mass Transit Modal Annex conformed to these requirements. We also analyzed executive guidance documents outlining best practices for effectively implementing a risk management framework, and in particular, risk assessment best practices, including both the DHS National Infrastructure Protection Plan (NIPP) and the TS-SSP. We also reviewed GAO best

¹ GAO and DHS reports on risk assessment include, but are not limited to, GAO, *Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts* GAO-05-851 (Washington, D.C.: September 2005) and the DHS National Infrastructure Protection Plan (NIPP).

practice criteria for developing a successful national strategy and compared the Mass Transit Modal Annex against it. Finally, to identify the extent to which TSA is measuring its performance in implementing its mass transit and passenger rail security programs, we reviewed DHS and TSA documents, including the Modal Annex, DHS Critical Infrastructure and Key Resources Annual Reports, and Surface Transportation Regulatory Activities Plan, as well as the Office of Management and Budget's Program Assessment Rating Tool (PART), which assessed the adequacy and effectiveness of these program measures.

To identify and describe the key actions federal and industry stakeholders have implemented or initiated since 2004 to strengthen the security of mass transit and passenger rail systems, the extent to which federal actions are consistent with TSA's security strategy, and the challenges, if any, that TSA has faced in making these actions effective, we interviewed officials from DHS and DOT. From DHS, we interviewed officials from TSA's Surface Transportation Security Inspection Program within the Office of Security Operations, TSA's Office of Security Technology, and, within TSA's Office of Law Enforcement, the Federal Air Marshal Service (which plays a lead role in implementing VIPR Operations). We also interviewed officials from DHS's Science and Technology Directorate and Federal Emergency Management Agency's Grants Programs Directorate. Within DOT, we interviewed officials from FTA's Office of Safety and Security and also the Federal Railroad Administration. We also interviewed officials from the three federally sponsored mass transit employee training providers—the National Transit Institute, Transportation Safety Institute, and Johns Hopkins University—to obtain information on training they offered to mass transit and passenger rail employees and their perspectives on TSA's Mass Transit Security Training Program.

To obtain information on industry security actions and perspectives on federal mass transit and passenger rail security actions, we conducted site visits at, or held teleconferences with, officials representing 30 mass transit and passenger rail systems across the nation—representing 75 percent of the nation's total mass transit and passenger rail ridership—based on information we obtained from the Federal Transit Administration's National Transit Database and the American Public Transportation Association (APTA). We selected this non-probability sample of mass transit and passenger rail systems and cities because of their high levels of ridership, geographic dispersion, experience with TSA security assessments, eligibility for grant funding, and expert recommendation. Because we selected a non-probability sample of mass

transit and passenger rail agencies, the information obtained from these site visits cannot be generalized to all transit agencies nationwide. However, we determined that the selection of these sites was appropriate for our design and objectives and that the selection would provide valid and reliable evidence. The information we obtained provided us with a broad overview of the types of actions taken to strengthen security. Table 1 lists the mass transit and passenger rail systems we interviewed.

Table 7: Mass Transit and Passenger Rail Systems Interviewed

Mass transit and/or passenger rail system	Urban area served
Bay Area Rapid Transit (BART)	San Francisco-Oakland, California
Broward County Office of Transportation (BCT)	Broward County, Florida
CALTRAIN	San Francisco and San Jose, California
Chicago Transit Authority (CTA)	Chicago, Illinois
Dallas Area Rapid Transit (DART)	Dallas, Texas
Delaware River Port Authority (PATCO)	New Jersey and Philadelphia, Pennsylvania
Fort Worth Transportation Authority (The T)	Fort Worth, Texas
King County Department of Transportation – Metro Transit Division (King County Metro)	Seattle, Washington
Los Angeles County Metropolitan Transportation Authority (LACMTA)	Los Angeles, California
Maryland Transit Administration (MTA)	Greater Washington, D.C., and Maryland
Massachusetts Bay Transportation Authority (MBTA)	Boston, Massachusetts
METRA Commuter Rail	Chicago, Illinois
Metropolitan Atlanta Rapid Transit Authority (MARTA)	Atlanta, Georgia
Metro Transit	Minneapolis, Minnesota
Metropolitan Transit Authority of Harris County (Houston Metro)	Houston, Texas
Miami Dade Transit	Miami, Florida
New Jersey Transit	Newark, New Jersey – New York, New York
New York Metropolitan Transit Authority (MTA)	New York, New York
Orange County Transportation Authority (OCTA)	Orange County, California
Pierce County Public Transportation Benefit Area (Pierce Transit)	Tacoma – Seattle, Washington

Mass transit and/or passenger rail system	Urban area served
Port Authority Trans Hudson (PATH)	New York, New York—New Jersey
Santa Clara Valley Transportation Authority (VTA)	San Jose, California
South Florida Regional Transportation Authority (SFRTA)	Miami, Florida
Southern California Regional Rail Authority (Metrolink)	Greater Los Angeles, California
San Francisco Municipal Railway (MUNI)	San Francisco, California
Sound Transit (Sounder)	Seattle, Washington
Southeastern Pennsylvania Transportation Authority (SEPTA)	Philadelphia, Pennsylvania
TRIMET	Portland, Oregon
Virginia Railway Express (VRE)	Northern Virginia, Greater Washington, D.C.
Washington Metropolitan Area Transit Authority (WMATA)	Washington, D.C.

Source: GAO and TSA data.

We also interviewed Amtrak headquarters officials and visited three Amtrak station locations in the Northeast Corridor. During site visits to mass transit and passenger rail agencies, we interviewed security officials, toured stations and other facilities such as control centers, and observed security practices. Further, we interviewed TSA surface transportation security inspectors from the 13 field offices responsible for overseeing the passenger rail and mass transit systems we visited, and in one case, observed the inspectors conduct a BASE review of a mass transit system. We also interviewed state officials with homeland security responsibilities, representatives of the American Public Transportation Association, and where applicable, regional transportation authority officials. To determine the extent to which federal and industry actions were consistent with TSA’s security strategy, we reviewed TSA and FTA documentation describing ongoing programs and compared them with the strategic objectives, programs, and actions TSA described in its Mass Transit Modal Annex.

To further assess federal and industry actions, and identify potential challenges, we reviewed DHS and DOT documents relevant to federal and industry stakeholder actions to secure passenger rail and mass transit systems. For example, we reviewed program documentation for TSA’s Mass Transit Security Training Program, as well as FTA’s 2009 Final Draft of Training Curriculum Development Guidelines and federal transit employee training curricula. We also reviewed TSA’s Surface

Transportation Security Inspection Program Standard Operating Procedures, strategic and annual plans, and documentation of completed mass transit and passenger rail security assessments. We also reviewed TSA's Concept of Operations (CONOPS) for its Visible Intermodal Prevention and Response (VIPR) program—TSA's program for deploying security personnel to augment security on mass transit and passenger rail systems—to identify guidelines TSA has established for implementing the program. We then obtained a list of VIPR operations, by location and date, that TSA reported conducting in mass transit and passenger rail systems immediately following its issuance of the CONOPS in October 2007. We obtained and matched this list with information found in electronic copies of all TSA VIPR operation plan after-action reports (AAR)—describing the results and challenges encountered during VIPR operations that TSA conducted at mass transit and passenger rail systems from November 2007 through July 2008. We chose to review after-action reports for this period to determine the impact of guidance TSA issued in October 2007, to improve its implementation of the VIPR program. Both the initial list and after-action reports identified 108 VIPR operations; however, we reviewed 104 of these.² Two analysts independently coded the challenges noted on each of the reports. They discussed differences until agreement could be reached on the most appropriate challenge category. We also conducted a site visit to the Transportation Security Operations Center to interview officials with TSA's Federal Air Marshal Service within the Office of Law Enforcement—which manages the VIPR program—to discuss the challenges identified in the after-action reports. We also obtained access to, and reviewed, the DHS Homeland Security Information Network - Public Transit Portal secure Web communication system to identify the type and extent of security technology information that TSA had made available to industry users of the system, and identified and reviewed best practices applicable to R&D programs identified by leading research organizations, such as the National Research Council of the National Academy of Sciences, in order to establish criteria for evaluating federal and industry coordination in research and development efforts. We also reviewed two DHS-IG reports and found the quality of the methods used to develop these reports sufficient for use as a source in this report.

² We did not review four after actions report files because they could not be opened or TSA did not provide a report that was associated with the operation on TSA's original list.

For the final objective, to determine the status of TSA's implementation of 9/11 Commission Act requirements for mass transit and passenger rail, and challenges, if any, that TSA and the mass transit and passenger rail industry face in meeting these requirements, we reviewed the 9/11 Commission Act to identify DHS and industry requirements related to mass transit and passenger rail security. We also reviewed TSA status reports outlining the agency's reported status in satisfying various 9/11 Commission Act provisions related to mass transit and passenger rail security. However, we did not verify the accuracy of TSA's reported status in implementing these 9/11 Commission Act requirements. To identify potential challenges TSA and the mass transit and passenger rail industry may face in implementing various 9/11 Commission Act requirements, we interviewed TSA headquarters officials from the Transportation Security Network Management—Mass Transit division, including the Deputy General Manager, and officials from TSA's Surface Transportation Security Inspection Program, including the headquarters based Program Chief, and Surface Transportation Security Inspectors from 13 of 54 field offices, including 11 of 12 Assistant Federal Security Directors for Surface.³ We also reviewed TSA program documents relating to its inspection program including strategic and annual inspection plans, standard operating procedures, and memorandums and directives documenting organizational and staffing plans. Moreover, to obtain information on industry perspectives of potential challenges, we interviewed officials from 30 mass transit and passenger rail systems and Amtrak as well as APTA. In addition, we obtained and reviewed various reports which discuss the federal or industry role in implementing the 9/11 Commission Act, including recent reports issued by the DHS-IG, Congressional Research Service, and a January 2008 report prepared by six Assistant Federal Security Directors for Surface.

We conducted this performance audit from September 2007 through June 2009 in accordance with generally accepted government auditing standards. Those 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 and conclusions based on our audit objectives.

³ We visited or conducted phone interviews with Surface Transportation Security Inspectors in each location where we visited a mass transit or passenger rail system and TSA had maintained a field office for the inspectors.

Appendix II: TSA/FTA Security and Emergency Management Action Items

The following list of voluntary Security and Emergency Management Action Items is an update to the Federal Transit Administration's Top 20 Security Program Action Items originally released in January 2003. The update has been developed by FTA and the Department of Homeland Security's Transportation Security Administration and Office of Grants & Training in consultation with the public transportation industry through the Mass Transit Sector Coordinating Council, for which the American Public Transportation Association serves as Executive Secretary. The updated action items address current security threats and risks that confront transit agencies, with particular emphasis on priority areas where gaps need to be closed in security and emergency preparedness programs. Though this update consolidates the previous 20 items into 17, the purpose, scope, and objectives remain consistent.

Management and Accountability

1. Establish written security plans and emergency management plans.
2. Define roles and responsibilities for security and emergency management.
3. Ensure that operations and maintenance supervisors, forepersons, and managers are held responsible for security issues under their control.
4. Coordinate security and emergency management plan(s) with local and regional agencies.

Security and Emergency Response Training

5. Establish and maintain a security and emergency training program.

Homeland Security Advisory System

6. Establish plans and protocols to respond to the DHS Homeland Security Advisory System threat levels.

Public Awareness

7. Implement and reinforce a Public Security and Emergency Awareness Program.

Drills and Exercises

8. Conduct tabletop and functional drills.

Risk Management and Information Sharing

9. Establish and use a risk management process to assess and manage threats, vulnerabilities and consequences.

	10. Participate in an information sharing process for threat and intelligence information.
	11. Establish and use a reporting process for suspicious activity (internal and external).
Facility Security and Access Controls	12. Control access to security critical facilities with ID badges for all visitors, employees, and contractors.
	13. Conduct physical security inspections.
Background Investigations	14. Conduct background investigations of employees and contractors.
Document Control	15. Control access to documents of security critical systems and facilities.
	16. Ensure existence of a process for handling and access to Sensitive Security Information (SSI).
Security Audits	17. Conduct security program audits.

Appendix III: Identifying Characteristics of Successful National Strategies in the Context of Mass Transit and Passenger Rail Security

To help the federal government develop sound national strategies, we have previously identified six desirable characteristics of successful national strategies, including (1) purpose, scope, and methodology of the strategy; (2) risk assessment; (3) goals, subordinate objectives, activities, and performance measures; (4) resources and investments; (5) organizational roles, responsibilities, and coordination; (6) integration and implementation.¹ We discussed four of these characteristics in the body of the report, and below we discuss the other two characteristics.² Where applicable, we link relevant sections of Executive Order 13416 to highlight the importance of these measures to strengthen the passenger rail and mass transit security national strategy.

Purpose, Scope, and Methodology

This characteristic addresses why the strategy was produced, the scope of its coverage, and the process by which it was developed. For example, a strategy might discuss the specific impetus that led to its creation, such as statutory requirements, executive mandates, or other events—such as terrorist attacks. In addition to describing what the strategy is meant to do and the major functions, mission areas, or activities it covers, a national strategy would ideally also outline its methodology. For example, a strategy might discuss the principles or theories that guided its development, what organizations or offices drafted the document, whether it was the result of a working group, or which parties were consulted in its development.

TSA’s Mass Transit Modal Annex identifies the purpose and scope of the Modal Annex and references several principle documents used to develop the Modal Annex—including the Presidential Executive Order 13416: *Strengthening Surface Transportation Security*, the Transportation System- Sector Specific Plan (TS-SSP), and the National Infrastructure Protection Plan. It also describes the process or methodology that was used and who developed the Annex. For example, the Modal Annex states that TSA’s vision is to provide a secure, resilient transit system that leverages public awareness, technology, and layered security programs while maintaining the efficient flow of passengers and encouraging the expanded use of the nation’s transit services. The Modal Annex also

¹ GAO-04-408T.

² In this report we discuss resources and investments; risk assessment; developing goals, subordinate objectives, activities, and performance measures; and identifying organizational roles, responsibilities, and coordination.

discusses the scope and type of various federal and industry mass transit and passenger rail security efforts and aligns them with three broad DHS security goals for the transportation sector, as outlined in the TS-SSP.³ In addition, the Modal Annex references the National Infrastructure Protection Plan as a source for developing security programs for mass transit and passenger rail systems, and it also discusses several domestic and international terrorist attacks that have occurred as evidence of the various security risks to the mass transit and passenger rail systems.⁴ Furthermore, the Modal Annex explains the methodology used in its development, as called for in our prior work on characteristics of a national strategy.

In addition to referencing the National Infrastructure Protection Plan and the TS-SSP as literatures providing the principles or theories that guided the development of the Modal Annex, the Modal Annex also describes the process and information that were used to develop the strategy and identified entities that contributed to its development. For example, the strategy describes how mass transit and passenger rail security programs and initiatives are developed and implemented and how they are aligned with the overall transportation sector goals and objectives and mass transit and passenger rail modal strategies and objectives. Also, the Modal Annex identifies the Transit, Commuter and Long Distance Rail Government Coordinating Council (TCLDR-GCC), the Mass Transit Sector Coordinating Council (SCC), the Critical Infrastructure Partnership Advisory Council, and TSA's Mass Transit Division as entities involved in developing the transportation security strategic policy.

Integration and implementation

This characteristic addresses both how a national strategy relates to other strategies' goals, objectives, and activities and to subordinate levels of government and their plans to implement the strategy. For example, a national strategy could discuss how its scope complements, expands upon, or overlaps with other national strategies, such as DHS efforts to mitigate transportation risks. Also, related strategies could highlight their common or shared goals, subordinate objectives, and activities. Similarly,

³These sector goals are: 1) prevent and deter acts of terrorism using or against the transportation system; 2) enhance the resiliency of the U.S. transportation system; and 3) improve the cost-effective use of resources for transportation security.

⁴These incidents include, but are not limited to the September 11, 2001, attacks on the World Trade Center and the Pentagon, coordinated attacks on four commuter trains in Madrid in 2004, and attacks on transportation targets in the 2005 London bombings and the 2006 train bombings in Mumbai.

the Executive Order requires that the Modal Annex identify existing security guidelines and requirements. To meet these requirements and because protecting the mass transit and passenger rail systems is a shared responsibility among many stakeholders, the Modal Annex could identify regulations and programs that affect the security of the mass transit and passenger rail systems. In addition, a strategy could address its relationship to other agency strategies using relevant documents from implementing organizations, such as strategic plans, annual performance plans, or annual performance reports that GPRA requires of federal agencies. A strategy might also discuss, as appropriate, various strategies and plans produced by the state, local, or private sectors and could provide guidance such as the development of national standards to more effectively link together the roles, responsibilities, and capabilities of the implementing parties.

TSA's Modal Annex delineates mechanisms to facilitate stakeholders coordination, specifically the TCLDR-GCC and the Mass Transit SCC, discusses other relevant industry security plans, and identifies regulations and programs such as the regulation on designating a rail security coordinator and security programs related to public awareness and training that affect the security of the mass transit and passenger rail systems. The Modal Annex also addresses its relationship with strategic documents or activities of other federal agencies that have a role in mass transit and passenger rail security, such as those that guide FTA, which has a supporting role along with TSA for protecting mass transit and passenger rail systems. For example, the Modal Annex mentions how FTA's activities, such as the State Safety Oversight Agencies audit program and FTA's Section 5307 grant program fit into TSA's overall strategy for securing mass transit and passenger rail systems. The Modal Annex also mentions DHS-DOT collaborative efforts through their memorandum of understanding such as the development of public transportation annex delineating areas of coordination to assist transit agencies in prioritizing and addressing security related needs. In addition, the Modal Annex points out how it relates to the National Strategy for Transportation Security required by the Intelligence Reform and Terrorism Prevention Act of 2004.⁵ For example, it explains how TSA's effort in building security force multipliers through security training for front-line employees of mass

⁵ The National Strategy for Transportation Security, required by section 4001 of the Intelligence Reform and Terrorism Prevention Act of 2004 outlines the federal government approach – in partnership with state, local and tribal governments and private industry – to secure the U.S. transportation system from terrorist threats and attacks.

transit and passenger rail systems directly supports the National Priorities, the National Preparedness Goal, and the National Strategy for Transportation Security. By providing such information, the agency is identifying linkages with other developed strategies and other organizational roles and responsibilities.

Appendix IV: Federal Actions Taken to Enhance Mass Transit and Passenger Rail Security since 2004

This appendix expands on the list of key actions identified in the body of the report in table 5. This table presents a more comprehensive list of federal actions taken to enhance mass transit and passenger rail security since 2004.

Table 8: Federal Actions Taken to Enhance Mass Transit and Passenger Rail Security since 2004

Category/program	Lead agency	Description
<i>Deploying Manpower</i>		
Surface Transportation Security Inspection Program (STSIP)	TSA	Established in 2005, TSA's Surface Transportation Security Inspectors (TSI-S) serve as the agency's field force for conducting non-regulatory security assessments, outreach, and technical assistance with the nation's largest mass transit agencies, as well as participating in VIPR security operations at key transit and passenger rail locations. TSA reported that, as of February 2009, TSI-S had conducted non-regulatory security posture assessments—BASE reviews—of 91 mass transit and passenger rail agencies, including 82 of the largest agencies, and over 1,350 site visits to mass transit rail stations—Station Profiles—to gather detailed information pertaining to their physical security elements, geography, and emergency points of contact.
Visible Intermodal Prevention and Response (VIPR) Program	TSA	TSA, to date, has reported deploying over 800 teams 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 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.
National Explosive Detection Canine Team Program (NEDCTP)	TSA	In 2005, TSA expanded the NEDCTP from aviation into mass transit. TSA has worked in partnership with mass transit systems to procure, train, certify, and deploy 88 explosives detection canine teams to 15 participating mass transit systems nationwide to provide mobile and flexible deterrence and explosives detection capabilities. TSA provides the canine training for the handler and the dogs and also allocates funds to cover costs associated with continued training and maintenance of the team, while the transit system commits a handler to attend the TSA training and receive program certification.
<i>Coordinating with federal and industry stakeholders and issuing guidance</i>		
Mass Transit Modal Annex	TSA	In 2007, TSA, in coordination with FTA, issued the Mass Transit Modal Annex to serve as the federal strategy for achieving the objectives and priorities laid out in the Transportation Systems-Sector Specific Plan. The Modal Annex outlines security programs and activities—initiated largely by TSA, but including FTA and other federal stakeholders—to enhance the security of the nation's mass transit and passenger rail systems.

DHS/DOT memorandum of understanding (MOU) for coordination of roles/responsibilities	TSA FTA	Through a 2004 MOU and 2005 annex DOT (FTA) and DHS (TSA) agreed to closely coordinate their mass transit and passenger rail programs and services in developing mass transit and passenger rail security guidance and regulations, with TSA as the lead agency. The agreements confirm TSA as having the lead role for transportation security and DOT as having a supporting role for providing technical assistance and assisting DHS in the implementation of its security policies.
Transit, Commuter and Long Distance Rail Government Coordinating Council and Mass Transit Sector Coordinating Council (GCC/SCC) Joint Working Groups	TSA FTA	In 2007, under the Transit, Commuter and Long Distance Rail Government Coordinating Council (GCC) and Mass Transit Sector Coordinating Council (SCC) framework, TSA and FTA collaborated with the American Public Transportation Association to establish working groups composed of federal and industry mass transit and passenger rail security stakeholders to serve as a modal coordinating council for the mass transit and passenger rail modes. Working groups were established in three substantive areas: security training, security technology, and grants.
Transit Policing and Security Peer Advisory Group (PAG)	TSA	In late 2006, TSA established the monthly Transit Policing and Security Peer Advisory Group (PAG) to bring together 16 transit police chiefs and security directors from Amtrak and major transit systems across the nation to act as a consultative forum for advancing the security concerns of transit systems.
Transit Safety and Security Roundtables	TSA FTA	Administered in 2003 and 2004 by FTA, and jointly administered since 2005, TSA and FTA have convened semi-annual Transit Safety and Security Roundtables to serve as a means for representatives of the 50 largest mass transit agencies to share security-related ideas and information.
Coordinated Security Surges	TSA	Coordinated effort integrating TSA with mass transit and passenger rail agencies and law enforcement partners in the systems' operating areas. TSA reported initiating the program with planning, coordination, and execution of "Northeast Corridor Rail Security Day" in September 2008, a surge operation that brought officers from nearly 120 law enforcement agencies to some 150 Amtrak, commuter rail, and rail transit stations from Fredericksburg, Virginia to Portland, Maine.
Security Standards	TSA FTA	In accordance with the DOT-DHS MOU annex, FTA is leading an initiative with TSA to develop security standards for mass transit and passenger rail systems, with a focus on recommended procedures and practices. FTA has funded APTA to administer this initiative, and as of March 2009, APTA had issued six security standards related to security emergency management, security infrastructure, and security risk management.
Smart Security Practices List	TSA	In June 2008, TSA disseminated to the mass transit industry a list of 55 smart security practices listing the most effective security activities, measures, practices, and procedures inspectors had identified in TSA mass transit security assessments. TSA plans to periodically expand this list as it continues to identify additional smart practices through its security assessments.

Mass Transit Security Training Program	TSA FEMA FTA	In early 2007, to improve the quality and scope of transit agency employee security training, TSA established the Mass Transit Security Training Program to provide transit agencies with curriculum guidance and expedited grant funding to cover training costs. FEMA administers the funding through the Transit Security Grant Program. The program is largely based on courses developed and financially supported by FTA. For example, among other things, FTA funds and supports delivery of a variety of security training, including 17 security training programs for mass transit and passenger rail agency employees.
Connecting Communities Public Transportation Emergency Preparedness Workshops	FTA TSA	Established by FTA in 2002 and funded by both FTA and TSA, these 2-day workshops are designed to facilitate coordination between federal stakeholders and the local agencies that respond to transit emergencies. TSA and FTA share transit policies, procedures, resources, and effective practices with local first responders and discuss emergency management and response, including the roles of federal, state, and local emergency management offices. FTA and TSA convene these workshops several times per year in cities nationwide.
Transit Watch	TSA/ FTA	To boost public vigilance and awareness of potential terrorist threats, Transit Watch was introduced in 2003 as a nationwide safety and security awareness program designed to encourage the active participation of transit passengers and employees. Via the program, TSA/FTA jointly created templates for use by transit agencies to produce security-awareness materials, such as posters and flyers.
Bomb Squad Response to Transportation Systems	TSA	TSA reported that through training and scenario-based exercises, this program expands regional capabilities to respond to a threat or incident involving a suspected explosive device in mass transit and passenger rail systems. Bomb technicians from law enforcement forces in the system's operating area are placed in the mass transit or passenger rail environment to confront exercise situations necessitating coordinated planning and execution of operations to identify, resolve, and, if appropriate, render harmless improvised explosive devices. TSA reported that as of May 2009, this program has been conducted at three mass transit locations.
Employee Awareness Program	TSA	TSA reported that this program produces posters and tip cards for frontline employees emphasizing the critical importance of observing and reporting in terrorism prevention. The products are adapted to the partnering agency, applying its logo, system images, and employees' quotes.
<i>Developing security technology and providing technology information</i>		
Security Technology Research and Development	DHS S&T/ TSA	DHS Science and Technology Directorate and TSA collaborate to research, develop, and test various security technologies for applicability in the mass transit and passenger rail modes, including explosive trace detection technologies, infrastructure protection measures, and behavior based and advanced imaging technologies.
Homeland Security Information Network Public Transit Portal	TSA	In 2006, TSA established the Public Transit Portal of the Homeland Security Information Network, a secure, web-based communications system to provide the mass transit industry with information on threats, best practices, and security technologies.

Transportation Research Board

FTA

FTA sponsors academic research from the Transportation Research Board (TRB), which is one of six divisions within the National Research Council. The National Research Council serves as an independent advisor to the federal government and others on scientific and technical questions of national importance. TRB has produced several reports on public transportation security, such as a report on mass transit passenger security inspections procedures and technology.

Source: GAO analysis of DHS and DOT information.

Appendix V: Modal Annex Objectives and Examples of Actions Taken to Achieve Them as of February 2009

Table 9: TSA Mass Transit Modal Annex Objectives and Examples of Actions That Have Been Employed to Achieve the Objectives, as of February 2009

Modal Annex mass transit objectives	Action to achieve objective
<ul style="list-style-type: none"> Employ technology for screening passengers and bags in random applications throughout the mass transit and passenger rail systems as appropriate. 	Explosive detection technology screening employed during VIPR operations
<ul style="list-style-type: none"> Bolster screening technology efforts with a program for random searches of passengers' bags entering system. 	Screening programs introduced by select major transit agencies
<ul style="list-style-type: none"> Affect regional approach through coordinated planning among federal, local, and mass transit security stakeholders to maximize application of available security resources through multiple teams for random, unpredictable activities. 	TSA VIPR operations and coordinated security surges
<ul style="list-style-type: none"> Conduct Security Readiness assessments. 	TSA BASE reviews
<ul style="list-style-type: none"> Coordinate with system security officials to examine capabilities of transit agencies and front-line employees in identifying and reporting suspicious items and activities. 	TSA Security Analysis and Action Program Assessments
<ul style="list-style-type: none"> Use covert testing to test awareness and reporting by employees and passengers. 	N/A ^a
<ul style="list-style-type: none"> Improve flow of threat and other security information through outreach and regional intelligence and information-sharing centers. 	Joint Terrorism Task Force mass transit threat briefings ^b and TSA mass transit security awareness messages ^c
<ul style="list-style-type: none"> Coordinate focused transit system employee training to be aligned with needs and requirements of mass transit agencies. 	TSA Mass Transit Security Training Program
<ul style="list-style-type: none"> Employ all available media-public address system announcements in public awareness programs. 	TSA Employee Awareness Poster Program ^d

Source: GAO Analysis of TSA information and Mass Transit Modal Annex.

^aAs of February 2009, due to potential safety risks and potential disruptions to transit operations, TSA has elected not to conduct covert testing of passenger rail and mass transit systems.

^bDHS, TSA, and the Federal Bureau of Investigation (FBI) conduct Joint Terrorism Task Force (JTTF) Mass Transit Threat Briefings on a quarterly basis, or as threats or security incidents warrant, bringing together mass transit and passenger rail security directors and law enforcement chiefs with their federal security partners in 15 metropolitan areas simultaneously through the secure video teleconferencing system maintained in the JTTF network.

^cThrough its Mass Transit Security Awareness Messages, TSA periodically disseminates unclassified threat information to mass transit and passenger rail security and management officials to increase vigilance and preparedness and practical guidance on how to enhance security.

^dThrough the Employee Awareness Poster Program, TSA partners with mass transit and passenger rail agencies to produce tailored posters specifically focused on transit employee security awareness. TSA develops a common theme, transit agencies provide graphics, logos, and quotations, and TSA tailors the posters for use by the transit agencies.

Appendix VI: DHS Mass Transit and Passenger Rail Related Security Technology Pilots Conducted from 2004 to 2009

Table 10: DHS Mass Transit and Passenger Rail Related Security Technology Pilots Conducted from 2004 to 2009

Pilot program	Description	Status
Program for Response Options and Technology Enhancement for Chemical/Biological Terrorism (PROTECT)	Technology is an automated network of chemical sniffers, TV cameras, and computers that provides early warning of chemical attack, as well as intelligent emergency response management.	Evaluation is completed. In March 2003, it became the nation's first permanently installed detection system for chemical attacks in a public place. PROTECT can be found in three major cities.
Transit and Rail Inspection Pilot (TRIP)	Three phase pilot program launched in 2004 that evaluated the feasibility of using checkpoint style passenger screening, explosive trace detection systems for passenger checked baggage, and evaluated the feasibility of modifying a passenger rail car by installing screening technologies within it and conducting passenger screening operations while the train was moving at normal speed.	Evaluation is completed. TSA found that the screening technologies and processes tested would be difficult to implement on more heavily used passenger rail systems. TSA concluded that the screening technologies could be used randomly or during certain high-risk events. For example, similar technologies were used by TSA to screen certain passengers and belongings in Boston and New York during the Democratic and Republican national conventions, respectively, in 2004.
Conventional screening technology adaptation pilot program (Countermeasures Test Beds Rail Security Pilot)	Congressionally mandated project which included testing the feasibility of adapting airport security checkpoint screening technologies and procedures to screen rail passengers and baggage for explosives and testing technologies that would be integrated into fare card purchasing machines to detect trace levels of explosive residue on the hands of passengers.	Evaluation is completed. Though DHS found that several of the technologies could be adapted to function on mass transit in the near term, it identified several obstacles that needed to be overcome, including high technology costs, high personnel requirements, high false-alarm rates, and reduced passenger throughput.
Mobile security checkpoints	Tested the rapid deployment of the "screener in a box" - a full airport-style x-ray checkpoint passenger and baggage screening system that fits into two standard-sized shipping containers.	Evaluation is completed. The pilot determined that the checkpoint could be used for screening passengers at a moderately busy transit platform, but coordination and logistical support, storage, screeners, and set-up challenges make these checkpoints suitable only for short term, high threat use in mass transit and passenger rail. The unit is now maintained for deployment in situations of heightened alert.
Advanced Screening Equipment - SPO-20 deployment	As part of TSA's increased security presence at the nation's major transportation centers on July 4 2007, TSA tested the rapid deployment of the SPO-20, a passive millimeter wave screening device that can scan large crowds for body-borne improvised explosive devices.	Evaluation is completed. TSA reported the pilot successfully screened almost all passengers at a busy transit station with few false alarms. The most significant challenge came from the fact that TSA gave the transit agency less than 24 hours to coordinate the SPO-20's deployment, which caused some logistical and training issues. TSA concluded that pre-deployment site visits and coordinating meetings are crucial to successful deployment.

Pilot program	Description	Status
Resilient tunnel	In 2003-2004, DHS S&T conducted an assessment of the nation's 29 underground and underwater tunnels for mass transit and passenger rail to identify ways to mitigate vulnerabilities that terrorists using improvised explosive devices could exploit to cause catastrophic failure of an underground transit tunnel.	Ongoing. In fiscal year 2007, the project surveyed concepts for tunnel protection and identified existing European inflatable tunnel protection systems that could be used to limit the spread of fire caused by an explosion. DHS S&T plans to complete and demonstrate a prototype inflatable tunnel protection system by fiscal year 2010.
Bus communications and control	In 2006, TSA and DHS S&T developed the ability to remotely disable a bus using engine control technologies and therefore prevent its use as a delivery device for a weapon of mass destruction.	Ongoing. In fiscal year 2007, the project began with full field operational testing, which will continue through fiscal year 2009.
Standoff technology demonstration program	A field testing program intended to accelerate the development of promising standoff detection technologies and adapted checkpoint screening systems. The program's objectives include testing and evaluating technologies, developing concept of operation plans, and to developing agile test beds to evaluate technologies.	Ongoing. In fiscal year 2010, the program will demonstrate an integrated system of technologies to detect a left-behind IED or a suicide bomber in commuter rail.
Future Attribute Screening Technologies Mobile Module (FASTM2)	This module is developing real-time, mobile screening technologies to automatically detect behavior indicative of mal-intent at security checkpoints such as border crossings, transportation portals, and other critical infrastructures.	Ongoing. In fiscal year 2009, the project plans to conduct a prototype demonstration of real-time intent detection capability.
Infrastructure Blast Mitigation Project	Project is developing proof-of-concept technologies to mitigate the explosive and damaging force from an IED. This project will include basic research studies on advanced mitigation technologies, including new glass materials and deflecting structures that reduce damage to infrastructure or personnel.	Ongoing. In fiscal year 2009, the project plans to begin developing models to further determine the vulnerability of infrastructure, bridges, and tunnels to various explosive threats.
Automated Carry-on Detection Project	Project develops advanced capabilities to detect explosives and concealed weapons, including home-made explosives. This project will introduce new standalone technologies or adjunct technologies to Computed Tomography technology to continue improving detection performance and the detection of novel explosives.	Ongoing. In fiscal year 2009, the project plans to award a development contract for the detection of novel explosives in what are called "next generation" checkpoint systems.

Pilot program	Description	Status
Concrete Mats for Tunnel Protection	Project is testing articulated concrete mats, which are composed of individual concrete blocks held together by a series of cables, for their potential effectiveness in protecting underwater transportation tunnels.	Ongoing. In fiscal year 2006, a series of scaled experiments in geotechnical centrifuge was initiated to evaluate the effectiveness of the mats for tunnel protection. In February 2009, the third phase of the experimental testing was nearing completion, after which a report will be generated. All work has been coordinated with a specific mass transit agency to inform the operational deployment of the mats once the project is finished.

Source: GAO analysis of TSA and DHS documents.

Appendix VII: Comments from Amtrak



June 15, 2009

Ms. Cathy Berrick
Managing Director
Homeland Security and Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Berrick:

Thank you for your correspondence of May 13, 2009, regarding a draft report from your office for "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-09-678SU" provided for agency comment.

With regard to industry stakeholders conducting risk assessments related to security, the Department of Homeland Security (DHS) funded a risk-based assessment of all Amtrak facilities, practices and assets in 2004-2005. DHS hired Science Applications International Corporation (SAIC) directly to conduct the assessment, which occurred from 2005 through 2008. The methodology employed conforms to DHS risk assessment standards. Amtrak has embraced this assessment as the baseline from which all subsequent security remediation priorities have been determined and acted upon.

In addition and since 2006, Amtrak has utilized corroborating sub-assessments, executed by institutions such as the Lawrence Livermore National Laboratories (LLNL), and the Department of Defense's (DOD) Full Spectrum Vulnerability Analysis Assessment (FSIVA) process, to confirm, augment, clarify, and otherwise round out the SAIC results.

TSA was largely uninvolved in this process, though the TSGP grant program administered by that agency did fund some of the sub-assessments.

In response to key remediation actions taken by industry stakeholders to address issues identified in risk-based assessments, Amtrak has taken and continues to aggressively implement remediation actions, in risk order priority, identified in the DHS-sponsored risk assessment, and in corroborating independent assessments. Broadly, these activities fall into the following categories:

- a) Physical infrastructure hardening (barriers, fences, CCTV systems, HVAC sensors, etc.) funded through successive Transportation Security Grant Programs (TSGP), and more recently through \$196 million from the ARRA.

Ms. Cathy Berrick
June 15, 2009
Page 2



- b) Employee and passenger security training and awareness programs funded in the same way.
- c) Increase in counter-terrorism security and police headcount, training, and capability, to include expansion of Amtrak's canine bomb detection program, through both grant and corporate operating budget funding.
- d) Prototype development of focused information sharing and intelligence systems, funded through grants.
- e) Development of station action teams and contingency plans for key facilities and stations (as identified by risk analysis), paid for through grants and corporate operating budget.

Detailed information on any or all of these programs can be made available upon written request.

TSA involvement in these activities is primarily that of a funding agency—in that it administers TSGP, first authorized by the Congress in 2005. Additionally, TSA has been significantly and profoundly helpful in the conduct of Amtrak security contingency operations and exercises since 2005.

DHS (through its Science and Technology Division) has been directly involved in assisting Amtrak with ideas and assessments of promising security technologies. TSA has sponsored exploratory tests with millimeter wave detection technologies.

Relating to impediments to implementing security remediation, the grants regime facilitates Amtrak's pursuit of security remediation (see above), especially with regard to physical infrastructure hardening.

The grant approval process managed by TSA and FEMA is at times cumbersome and overly bureaucratic. As well, the grant guidance administered by TSA sometimes diverged from clear legislative intent. This was particularly the case in the 2008 TSGP grant rules, which imposed a 25% cost share on grant funds selectively applied to five programs where Amtrak was implementing risk mitigation measures. While subsequently removed by Congressional action, this requirement caused hardship to transit agencies with already constrained resources, and considerable frustration to those charged with planning and scheduling complex projects distributed over multiple fiscal years.

We appreciate this opportunity to provide more detailed information on our security and counter-terrorism activities, and believe that the report contributes significantly to understanding the challenges involved in securing the transit environment.

Sincerely,

A handwritten signature in dark ink, appearing to read "J. Boardman", written over a light blue horizontal line.

Joseph H. Boardman
President and Chief Executive Officer

Appendix VIII: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

June 17, 2009

Ms. Cathleen A. Berrick
Managing Director, Homeland Security and Justice Issues
U.S. Government Accountability Office (GAO)
441 G Street, NW
Washington, DC 20548

Dear Ms. Berrick:

Thank you for the opportunity to comment on GAO-09-678SU, the draft report entitled, "Key Actions Have Been Taken to Enhance Mass Transit and Passenger Rail Security, but Opportunities Exist to Strengthen Federal Strategy and Programs." We commend the professionalism and thoroughness of the GAO team consistently displayed throughout the audit. The findings and recommendations in the report will prove helpful as we continue the persistent effort to strengthen the security strategy and enhance security programs for mass transit and passenger rail.

In particular, we appreciate the description of the extensive progress that has been made in security strategy, program development, and program execution since the publication of the last comprehensive GAO audit of mass transit and passenger rail in September 2005. As the report shows, TSA has developed a foundation for strong mass transit and passenger rail security. Constant commitment to improvement of this foundation is essential to meeting the challenges of the security mission. The current draft GAO report, which provides a broad investigation and pointed analysis, will foster this process.

Specific responses to the recommendations for executive action follow.

Recommendation 1: To help ensure that the federal strategy to secure the mass transit and passenger rail systems considers assessment information within the context of risk, TSA, as the Sector-Specific Agency for mass transit and passenger rail, should conduct a risk assessment that integrates all three elements of risk: threat, vulnerability, and consequence. As part of this assessment, TSA should, to the extent feasible, fully leverage existing assessment information from its own sources as well as those provided by other federal and industry stakeholders, as appropriate, and use this information to inform its security strategy.

DHS Concurs: We appreciate the constructive review and discussion of the subject of a comprehensive risk assessment in mass transit and passenger rail. In this context, it is important to note that mass transit and passenger rail agencies operating in the Nation's

- 2 -

sizeable metropolitan areas are among the most thoroughly assessed of all transportation modes. Since 9/11, they have undergone security assessments by the Federal Transit Administration (FTA), the former Office of Grants and Training of the U.S. Department of Homeland Security (DHS) (for grant funding eligibility), the American Public Transportation Association (APTA), private sector security consultants (often funded by DHS grants), and now the Baseline Assessment for Security Enhancement (BASE) program. Additionally, through DHS's Office of Infrastructure Protection, Protective Security Advisors (PSAs) have conducted risk assessments on specific critical assets in mass transit and passenger rail systems (including Amtrak) in higher risk areas.

As the draft report notes, through the BASE program, TSA assesses the security posture of mass transit and passenger rail agencies in the Security and Emergency Management Action Items. Developed in a joint effort of TSA, DHS, Department of Transportation/FTA, and mass transit and passenger rail operating and security officials engaged through the Mass Transit Sector Coordinating Council (SCC), the Action Items cover a range of areas that are foundational to an effective security program. Components include security program management and accountability, security and emergency response training, drills and exercises, public awareness, protective measures for Homeland Security Advisory System (HSAS) threat levels, physical security, personnel security, and information sharing and security. Particular emphasis is placed on posture in the six Transit Security Fundamentals (protection of underground/underwater infrastructure; protection of other high consequence systems and assets; random, unpredictable deterrence; training; exercises; and public awareness).

TSA's approach with the BASE program is distinct from the multiple risk assessments conducted previously in mass transit and passenger rail. The specific purpose is to evaluate, with a thorough checklist and narrative responses, the effectiveness of the security programs, procedures, and measures developed and implemented by mass transit and passenger rail agencies in response to the results of the prior risk assessments. TSA's Surface Transportation Security Inspectors (STSIs) conduct the BASE assessments in partnership with mass transit and passenger rail agencies' security chiefs and directors to ensure full understanding of their efforts and thorough assessment of their effectiveness.

The results of these assessments inform development of risk mitigation priorities, security enhancement programs, and resource allocations, including transit security grants. The results have also enabled production and dissemination of a compilation of Smart Security Practices, listed by implementing agency with name and contact information for a key official, with the specific purpose of inspiring networking among transit security professionals to expand adoption of these effective security practices. TSA disseminated the initial compilation to the mass transit and passenger rail community in July 2008. Annual updates are projected.

The assessed agencies receive a complete report of the results. This information helps focus the development and implementation of plans, programs, and measures to redress identified weaknesses and informs the preparation of project applications under the Transit Security Grant Program.

TSA acknowledges the importance of GAO's recommendation to leverage the results of these assessments and advance the capability to produce a comprehensive risk assessment of the

- 3 -

mass transit and passenger rail mode. The ongoing development of the Risk Assessment Tool, cited in Table 2 of the draft report, aims to provide a comprehensive risk assessment product for TSA in mass transit and passenger rail. A pilot program planned for later this year will apply this tool, evaluate its effectiveness, and produce lessons learned to enhance the capability prior to programmatic implementation. This effort, integrating the findings of the earlier assessments, is specifically intended to address this GAO recommendation.

Recommendation 2: To better achieve the security strategy laid out in its Mass Transit Modal Annex – TSA’s security strategy for the mass transit and passenger rail systems – TSA should, to the extent feasible, incorporate in future updates of the Modal Annex the characteristics of a successful national strategy and the elements outlined in Executive Order 13416, including:

- Measuring the agency’s and industry’s performance in achieving the goals of preventing and deterring acts of terrorism and enhancing the resiliency of mass transit and passenger rail systems; and
- Incorporating information on what the strategy will cost along with the sources and types of resources and investments needed, and identifying where those resources and investments should be targeted.

DHS Concurs: We welcome the constructive review and insights on improving the effectiveness of the Mass Transit Modal Annex to the Transportation Systems Sector-Specific Plan (TS-SSP) as TSA’s security strategy for mass transit and passenger rail. TSA will apply this context in the ongoing effort to update the Annex and enhance its utility as a national strategy. Additionally, TSA will coordinate this update with the mass transit and passenger rail community through multiple forums, such as the Mass Transit SCC, the Transit Policing & Security Peer Advisory Group, and participants in the semi-annual Transit Safety and Security Roundtables that bring together the law enforcement chiefs and security directors of Amtrak and the largest 50 mass transit and passenger rail agencies with federal security partners to advance collaborative solutions to security challenges.

Recommendation 3: To help ensure that DHS security technology research and development efforts reflect the security technology needs of the nation’s mass transit and passenger rail systems, TSA should expand its outreach to the mass transit and passenger rail industry in the planning and selection of related security technology research and development projects.

DHS Concurs: While we believe significant progress has been made in this area, as discussed in the draft report, the reference to concerns reported by the security technology working group of the Mass Transit SCC warrants our attention. As part of the continuous improvement process, we will strive to ensure security partners in mass transit and passenger rail are afforded ample and clear opportunities to provide input on priorities for security technology development and testing.

Recommendation 4: To meet the needs of mass transit and passenger rail agencies regarding information on available security technologies, TSA should explore the feasibility of expanding the security technology product information on the Public Transit Portal of the Homeland Security Information Network, and consider including information such as product performance in a rail or bus venue, cost, maintenance needs, and other information to support mass transit and passenger rail agencies purchasing and deploying new security technologies.

- 4 -

DHS Concurs: As noted in the discussion on this subject above, we recognize the need for a more comprehensive and user-friendly approach in providing appropriate information on security technologies that may be deployed in mass transit and passenger rail. To progress in this area, and consistent with the provisions of section 1410(b) of the 9/11 Commission Act, TSA has arranged funding in the amount of \$600,000 for operations of the Public Transportation Information Sharing and Analysis Center (PT-ISAC) in fiscal year 2009. Beyond meeting the statutory requirement, a principal objective of this initiative is to align and integrate the PT-ISAC's analytical and information sharing activities with relevant Federal processes to establish and maintain a comprehensive information sharing environment for the mass transit and passenger rail community. Expanding the scope and enhancing the quality of the security technology information resource, in coordination with the Mass Transit SCC, will be a key component of this effort.

Recommendation 5: To better ensure the 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 they could be used by transit agencies for training under the transit security grant program. As part of this effort, TSA should consider coordinating with other federal agencies that have developed criteria for similar programs, such as the Federal Transit Administration.

DHS Concurs: In recent years, DHS has substantially increased the investment in security training in mass transit and passenger rail through awards under the Transit Security Grant Program (TSGP). Though to date, new proposals for approval of courses for use of TSGP funds have been limited, we must anticipate growth in these types of requests from security training vendors as security training of frontline employees in mass transit and passenger rail remains a strategic security priority. An existing joint working group staffed by the appropriate officials from TSA and FTA is evaluating the security training program for mass transit and passenger rail to assess the effectiveness of current courses and to identify any gaps and needed improvements. Consistent with this GAO recommendation, we will add the establishment of criteria to review new training courses proposed by security training vendors to the joint working group's focus areas.

Recommendation 6: To better ensure DHS's ability to satisfy the provisions of the 9/11 Commission Act related to mass transit and passenger rail, DHS should develop a plan with milestones for implementing provisions of the 9/11 Commission Act related to mass transit and passenger rail security.

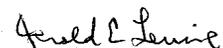
DHS Concurs: TSA reports its progress in implementing the requirements of the 9/11 Commission Act to DHS on a monthly basis. For items not yet completed, this monthly report includes projected actions to advance implementation with general timelines. However, a progress report is not the equivalent of an overall plan that identifies necessary actions and sets milestones to evaluate the effectiveness of efforts to meet the statutory requirements. Pursuant to this recommendation, TSA will produce such a plan.

**Appendix VIII: Comments from the
Department of Homeland Security**

- 5 -

Again, DHS appreciates the work GAO has done in the review of mass transit and passenger rail security. We look forward to maintaining communication with GAO as we work to continue progress in these areas.

Sincerely yours,


Jerald E. Levine
Director, DHS GAO/OIG Liaison Office

Appendix IX: GAO Contacts and Staff Acknowledgments

GAO Contacts

Cathleen Berrick, (202) 512-3404 or berrickc@gao.gov

Staff Acknowledgments

In addition to the contact named above, Dawn Hoff, Assistant Director, and Daniel Klabunde, Analyst-in-Charge, managed this assignment. Jay Berman, Martene Bryan, Charlotte Gamble, and Su Jin Yon made significant contributions to the work. Chuck Bausell and Rudy Chatlos, assisted with design, methodology, and data analysis. Lara Kaskie and Linda Miller provided assistance in report preparation; and Tracey King provided legal support.

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

