DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

# TSA's Administration and Coordination of Mass Transit Security Programs

OIG-08-66

June 2008

*Office of Inspector General*

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

Homeland Security

June 12, 2008

# Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the Homeland Security Act of 2002 (*Public Law 107-296*) by amendment to the Inspector General Act of 1978. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the department.

This report addresses the strengths and weaknesses of the Transportation Security Administration's (TSA) oversight and assistance programs for mass transit rail, including the Surface Transportation Security Inspection Program, the Transit Security Grant program, the Visible Intermodal Prevention and Response (VIPR) program, and the National Explosives Detection Canine Team Program. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, and a review of applicable documents.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. It is our hope that this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

Richard L. Skinner
Inspector General

# Table of Contents/Abbreviations



## Appendices



## Abbreviations

| | |
|---|---|
| BASE | Baseline Assessment for Security Enhancement |
| CBRNE | Chemical, Biological, Radiological, Nuclear, and Explosive |
| DHS | Department of Homeland Security |
| DOT | Department of Transportation |
| FEMA | Federal Emergency Management Agency |
| IED | Improvised Explosive Device |
| NEDCTP | National Explosives Detection Canine Team Program |
| OIG | Office of Inspector General |
| TSA | Transportation Security Administration |
| TSIs | Transportation Security Inspectors – Surface |
| TSNM | Transportation Sector Network Management |
| VIPR | Visible Intermodal Prevention and Response |

## Executive Summary

The *Aviation and Transportation Security Act of 2001* gave the Transportation Security Administration (TSA) responsibility for security on all modes of transportation. Following the Madrid train bombings of 2004, Congress directed TSA to administer transit security grants and to deploy federal rail compliance inspectors and canine explosive detection teams onto rail systems. Congress further clarified TSA's oversight role and operational mandate in mass transit with the *9/11 Commission Act of 2007*. Since 2004, TSA has initiated several programs to boost mass transit security. Our review focused on TSA's management of its four major assistance programs and how well these programs meet the needs of the nation's five largest mass transit rail systems.

TSA is improving mass transit security. It increased communication with transit stakeholders, entered into agreements with the Department of Transportation, and issued a sector-specific security plan. TSA initiated four major programs designed to mitigate vulnerabilities in mass transit rail systems. TSA created the Surface Transportation Security Inspection Program to comply with a Congressional mandate and to help rail transit systems identify and mitigate security vulnerabilities. TSA's Transit Security Grant Program funds local security projects. TSA augments transit security forces through the Visible Intermodal Prevention and Response program. TSA also oversees the training and deployment of canine explosive detection teams for rail.

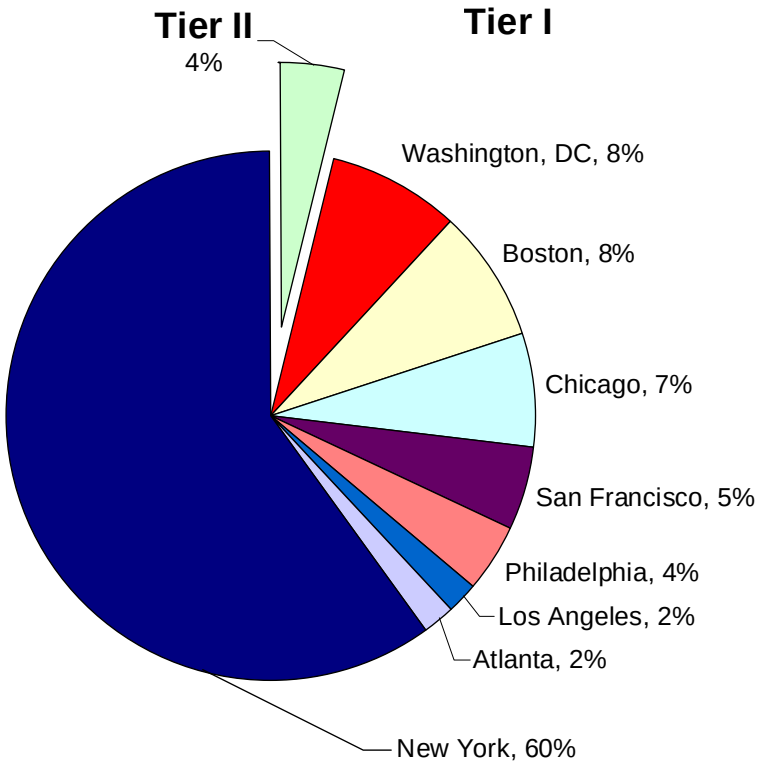
TSA faces important challenges to improve transit rail security, meet the needs of mass transit authorities, and comply with recent legislation, which expanded TSA's statutory authority and responsibility. TSA still needs to clarify its transit rail mission and develop additional regulations. It should develop memorandums of understanding with local transit authorities. TSA needs to improve inter-office communication and coordination. TSA also needs to understand and address system-specific security requirements better. We are making seven recommendations to improve management and coordination of mass transit rail security programs. TSA concurred with two recommendations, partially concurred with three, and did not concur with two. We incorporated TSA's response to our recommendations in Appendix B.

# Background

## Mass Transit Rail Systems in the United States

Mass transit rail systems, which include subways and commuter rail, are an essential part of the United States transportation infrastructure, providing more than 12 million passenger trips each workday. Although many cities have mass transit rail systems, 96% of the nation's passenger rail trips occur in eight metropolitan areas. The New York metropolitan area is the most heavily reliant on mass transit rail, accounting for 60% of all rail trips. The Washington, D.C., area has the second largest transit system, accounting for 8% of daily rail trips. The Department of Homeland Security (DHS) designates eight major urban areas with mass transit systems as Tier I, and the rest of the country's urban areas as Tier II (see Figure 1).

**Figure 1: Urban Area Share of Mass Transit Rail Passenger Trips**




**Source: American Public Transportation Association, 2005 Factbook**

As recent overseas attacks have shown, subway and commuter rail systems are inherently vulnerable to terrorism. A large system can have more than 100 stations, each with multiple station entrances and platforms, providing a terrorist numerous options for carrying out an attack. Passengers routinely wear bulky outdoor clothing and carry a variety of

packages or bags on board, which gives terrorists an easy way to conceal weapons or explosives. Limitations in current technology make screening millions of commuters impractical, and existing chemical and biological weapon sensors are only useful after an attack has already begun.

## Transportation Security Administration's Authority in Mass Transit Rail Security

The Transportation Security Administration (TSA) has authority and responsibility for security on all modes of transportation. Congress, DHS, and the Department of Transportation (DOT) have taken steps to address mass transit vulnerabilities and have enacted several directives and regulations (see Figure 2). These legislative and regulatory authorities give TSA broad powers, including the ability to inspect mass transit systems and deploy federal personnel onto transit systems during periods of increased threat. Most of these documents stress the importance of continued consultation and coordination with local mass transit operators.

**Figure 2: TSA Directive, Agreements, and Regulations**

**TSA Authority In Mass Transit Rail**

**November 19, 2001:** ***Aviation and Transportation Security Act.*** Gives TSA responsibility and authority over "security on all modes of transportation." TSA retains this authority when transferred to DHS on March 1, 2003.

**May 20, 2004: Security Directives.** Sets requirements for mass transit security, including designation of a Security Coordinator and TSA access to vulnerability assessments.*

**September 28, 2004: Memorandum of Understanding Between DHS and DOT.** Gives DHS the overall lead for transportation security, but specifies that DOT retain some responsibilities. Both parties must coordinate when drafting security regulations, funding security projects, and sharing intelligence.

**October 18, 2004:** ***Department of Homeland Security Appropriations Act of 2005*****.** Establishes the Surface Transportation Security Inspection Program. TSA Transportation Security Inspectors conduct voluntary baseline security assessments and serve as liaisons and advisors for mass transit systems. Authorizes the use of TSA canines for rail systems and transfers grant allocations to TSA.**

**September 8, 2005: Annexes to the Memorandum of Understanding Between DHS and DOT.** Requires TSA and DOT to collaborate on a number of security matters, including the establishment of public transportation security standards with participation from transit stakeholders.

* Security Directive SD RAILPAX-04-01, May 20, 2004
** Public Law 108-334, (2004); House Report 108-774 (2004)

**December 21, 2006: TSA Rail Security Regulations (pending final approval).** Establishes DHS' authority to access transit systems and their records without advance notice or observance of system requirements for safety training or identification. Requires immediate transit system notification to TSA regarding specific threats and security concerns.***

**May 21, 2007: TSA's Transportation Sector Specific Plan.** As required by Executive Order 13416, the Transportation Sector Specific Plan Mass Transit Annex identifies the following security goals: 1) expanding partnerships; 2) advancing the security baseline; 3) building security force multipliers; 4) providing information leadership; and 5) mitigating high consequence risk.

**August 3, 2007: *Implementing Recommendations of the 9/11 Commission Act of 2007*.** Introduces standards on the role of Transportation Security Inspectors, regulatory compliance, stakeholder relations, grants, Visible Intermodal Prevention and Response teams and TSA explosive detection canines.****

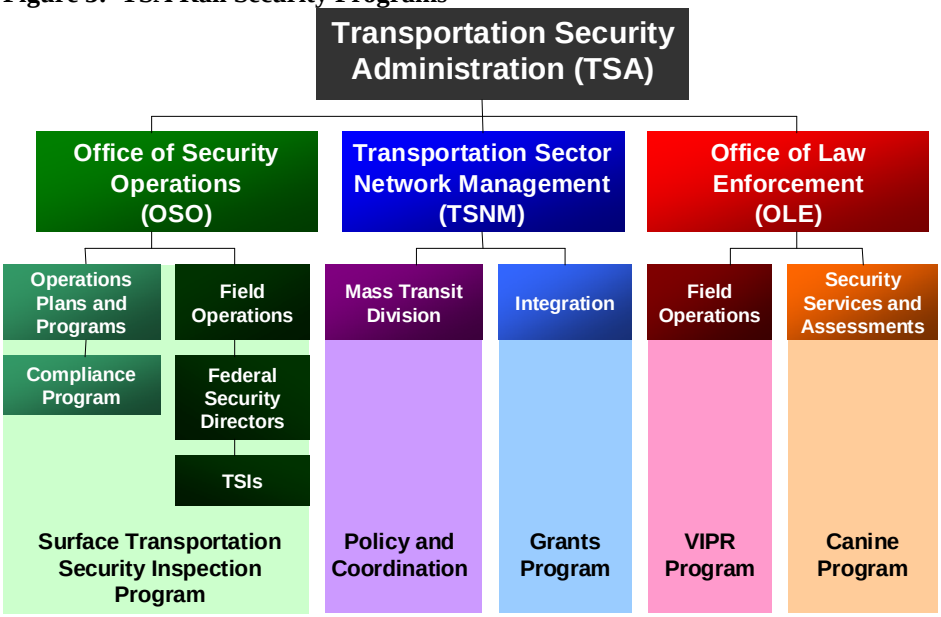
*** Pending regulatory changes 49 CFR Parts 1520 and 1580, Rail Transportation Security; Proposed Rule, December 21, 2006, 49 CFR § 1580.5
**** Public Law 110-53 (2007)

## TSA's Transit Rail Security Programs

TSA has created several programs to improve mass transit rail security. The Surface Transportation Security Inspection Program deploys roughly 100 Transportation Security Inspectors – Surface (TSIs) across the country. TSA also provides assistance to mass transit rail systems through the Transit Security Grant Program, the Visible Intermodal Prevention and Response (VIPR) program, and the National Explosives Detection Canine Team Program (NEDCTP).

Within TSA, the Office of Security Operations directs the Surface Transportation Security Inspection Program and sends instructions to the TSIs through the federal security directors, to whom the TSIs report. Transportation Sector Network Management (TSNM) sets policy for all modes of transportation. TSNM's Mass Transit Division develops strategies, policies, and programs to improve transit security including operational security activities, training exercises, public awareness, and technology. TSNM's Integration division administers the Transit Security Grant Program, and both Integration and Mass Transit focus on seven Transit Security Fundamentals (see Appendix D). The Office of Law Enforcement operates the VIPR program, though it shares this responsibility with the Office of Security Operations and TSNM. The Office of Law Enforcement also provides TSA explosive detection canines to transit systems (see Figure 3).

**Figure 3: TSA Rail Security Programs**




## Surface Transportation Security Inspection Program

Throughout 2005, the Surface Transportation Security Inspection Program deployed about 100 TSIs to field offices across the country. Their purpose was to inspect passenger rail systems and to review compliance with existing security standards and directives. The mission and organization of the TSIs has changed since the program's creation.

TSIs act as assessors, advisors, and liaisons. In mass transit systems, TSIs primarily perform Baseline Assessment for Security Enhancement (BASE) assessments. These assessments collect detailed information regarding a rail system's implementation of TSA and DOT recommended security measures. TSIs help increase TSA's knowledge of rail systems by responding to security incidents and by producing detailed profiles of a station's security features (station profiles). TSIs act as regional liaisons for transit systems and can advise systems on the use of grant funds. They also participate on VIPR teams. TSIs report to a federal security director, generally the top TSA official at an airport, who may also task them with nonsurface-related activities.

## Transit Security Grant Program

According to the American Public Transportation Association, most mass transit systems cannot cover their operational costs from passenger fares, and must rely on local taxes and federal grants. TSA's transit security grants are vital for funding

infrastructure hardening projects, technology, training, and operational costs for police patrols and explosive detection canine teams. The process for awarding transit security grants has changed every year since 2003 and continues to evolve. In addition to TSA grants, transit systems are eligible for other DHS security grants, and may use a small amount of DOT Federal Transit Administration grant money for security projects.

Fiscal year 2007 Transit Security Grants exceeded $270 million and TSA is required to allocate these funds based on a risk-management approach. TSA allocates funds to metropolitan regions based on a risk assessment formula that includes intelligence and threat analysis, the number of passenger trips, the number and length of underwater tunnels, and other factors. TSA then approves individual projects through negotiations with each area's Regional Transit Security Working Group, which includes state homeland security officials and chiefs of security from major transit systems. Funds are distributed with the help of the Federal Emergency Management Agency and the State Administrative Agencies.

## Visible Intermodal Prevention and Response Teams

Since the July 2004 Democratic National Convention in Boston, TSA has provided supplemental personnel to assist mass transit systems during major events, holidays, and anniversaries of prior attacks. These TSA personnel deploy as VIPR teams, whose goal is to provide a random, unannounced, unpredictable, high-visibility presence in a mass transit or passenger rail environment. The level of assistance transit systems request depends on a transit system's local political and security environment. A VIPR team may combine various types of TSA assets and perform an assortment of duties. One city used TSA screeners to augment local police screeners in random checks of passenger bags. Another city teamed federal air marshals and local transit police detectives in civilian clothes to observe crowds. Smaller systems have deployed TSA officials onto trains and buses to patrol with local police and canine teams. Beginning in July 2007, TSA significantly increased the number and frequency of VIPR deployments, from an average of one exercise per month to one or two exercises per week.

## National Explosives Detection Canine Team Program

In late 2005, TSA began offering the NEDCTP to mass transit rail systems. This program trains and certifies explosive detection canine teams, which consist of one TSA-owned canine and one

local law enforcement officer. The teams conduct random patrols, search unattended packages, and assist at explosive detection checkpoints.

As of September 2007, TSA had deployed approximately 50 teams to 14 mass transit systems across the nation. All teams undergo an initial 10-week training course at the Lackland Air Force Base near San Antonio, Texas. Following the training, teams return to their transit systems to patrol, search for explosives, and provide a visible deterrent. Teams train continuously and are recertified annually to ensure sustained performance. In addition to the donated canine and free training, the program provides participating agencies an annual stipend of $40,000 per team. In return, participating transit agencies agree to make their teams available for temporary duty in other facilities or cities during periods of heightened alert, provided the agency can spare its resources.

## Implementing Recommendations of the 9/11 Commission Act

The *Implementing Recommendations of the 9/11 Commission Act of 2007* (the *9/11 Commission Act*) included several provisions on mass transit rail security oversight and assistance that affect TSA's four major rail programs.[1] These provisions reinforce certain mission priorities and add some new direction.

The *9/11 Commission Act* requires Transportation Security Inspectors to assist mass transit systems with enhancing security and to possess relevant transportation experience. The Act requires TSIs to conduct compliance inspections and enforce applicable security regulations and directives. Security standards and mission must be consistent with agreements between DHS and DOT. TSA must consult with surface transportation entities on TSIs' duties, responsibilities, authorities and mission, and on strategies to improve transportation security and ensure compliance with security requirements. *The 9/11 Commission Act* prohibits DHS from issuing fines to mass transit agencies unless the agency is in violation, DHS has sought corrective action through written notice, and the agency does not take corrective action or propose an acceptable alternative means of compliance within a reasonable amount of time.[2]

[1] Public Law 110-53 (2007)
[2] Ibid.

TSA must submit an annual report to Congress on how its Transit Security Grants accomplish DHS' transportation security goals.[3] Prior to VIPR deployments, TSA is required to consult with local officials to agree on operational protocols, provide relevant information about the mission of the team, and consult with all transportation entities directly affected by the deployment.[4] The NEDCTP shall create certification standards for canines that TSA has not trained.

# Results of Review

The *Aviation and Transportation Security Act of 2001* gave the Transportation Security Administration authority and responsibility for security on all modes of transportation. Congress further clarified TSA's oversight role with the *9/11 Commission Act*. Beginning in 2004, TSA has increased its efforts to mitigate the vulnerability of mass transit rail systems across the United States. This has been accomplished by: introducing mass transit stakeholder security forums; developing guidance, memorandums and directives; using its Surface Transportation Security Inspection Program to provide voluntary vulnerability assessments; and providing support through grants and direct operational assistance.

TSA can improve certain aspects of each of their mass transit security programs. We observed: unclear or unduly complex chains of command; an unclear mission or insufficient guidance; and insufficient communication. TSA needs more consistency in its interactions with mass transit rail stakeholders, although it has acknowledged and attempted to address some early missteps that strained stakeholder relationships. Nonetheless, TSA should further integrate stakeholder expertise to effectively implement its oversight and assistance programs and fulfill its responsibility for mass transit security.

## TSA's Inspection Program Needs a Clear Mission and Command Structure

### Surface Transportation Security Inspection Program's Mission Needs Clarification

TSA has the authority to assess threats to transportation and enforce security-related regulations. Because comprehensive security regulations do not exist for mass transit, TSIs are hindered in carrying out this mission and providing formal oversight of mass

[3] Public Law 110-53 (2007)
[4] Ibid.

transit rail. A compliance element would strengthen TSIs' primary assessment work. By working with stakeholders to develop practical, enforceable, security standards, TSA can develop a clearer mission for its TSIs and begin to fulfill its responsibility for providing oversight to mass transit rail security.

At its inception, TSA envisioned the Surface Transportation Security Inspection Program to be a compliance program. The *2005 DHS Appropriations Act* created the program and called for the deployment of up to 100 federal rail compliance inspectors. TSA drafted a standard operating procedure for the program in April 2005, which listed monitoring compliance with the May 20, 2004, Security Directives as the program's primary mission. In response to the Security Directives, stakeholders complained that TSA did not properly consult them during the development phase. Stakeholders criticized the directives as being broad, costly, and contradictory to DOT safety standards. Additionally, TSIs had no easy recourse in the event of stakeholder noncompliance. As a result, TSA withdrew from its attempts to enforce the 2004 Security Directives, and instead pursued a strategy that emphasized collaboration on security enhancement instead of enforcement.

Because of this new strategy, the Surface Transportation Security Inspection Program focused on several initiatives. The 2007-2008 Strategic Plan for the program states that the TSIs' primary mass transit responsibility is to conduct BASE assessments. Field performance reports confirm that a majority of TSI time devoted to mass transit rail focuses on these assessments and on station profiles. In addition to the assessment mission, TSIs act as local liaisons, respond to local security incidents, and act as subject matter experts. TSIs participate in VIPR exercises and some receive non-surface transportation related tasks from their federal security director.

We conducted a survey of all current TSIs. In our survey, 30% of TSIs agreed that their mission and role in surface transportation security are clearly defined (see Appendix E for more details on the TSI survey). With regard to the BASE assessments and station profiles that TSIs produce, 75% of respondents said that mass transit systems believe such information is helpful, and 67% had raised security concerns that transit systems tried to address.

However, many mass transit stakeholders questioned the usefulness of TSIs' assessments because transit systems did not have the resources to address vulnerabilities identified in the assessments. Although most mass transit stakeholders spoke

highly of the professionalism and experience of many of the TSIs they worked with, most were not certain how TSA was using the information that TSIs were gathering. Most stakeholders said that they had participated in many different TSA assessments and system reviews, but unless such assessments were tied to grant funding to address the vulnerabilities that TSIs had identified, they had limited value.

Additionally, a few TSIs said that governing boards of mass transit systems were not motivated to address vulnerabilities and therefore TSIs needed compliance standards as a way to effect change. In our survey, 84% of TSIs believed that the authority to issue citations for violations of security regulations was necessary to do their job effectively. The *9/11 Commission Act* gave DHS authority to issue fines to mass transit agencies if the agency is found to be in violation, DHS has sought corrective action in writing, and the agency does not make acceptable changes.[5]

Compliance, assessments, and stakeholder support are all missions of the TSI program. The *9/11 Commission Act* states that TSIs should be used to "assist surface transportation carriers, operators, owners, entities, and facilities to enhance their security against terrorist attack and other security threats and to assist the Secretary in enforcing applicable surface transportation security regulations and directives."

However, TSA still has not developed specific comprehensive compliance regulations for mass transit systems to follow and TSIs to enforce. The September 8, 2005, Annex to the Memorandum of Understanding between DHS and DOT requires TSA and DOT to consult with one another to establish regulations and security standards for transit systems with participation from appropriate transit stakeholders. The parties have agreed to update standards over time, taking into account information on available technologies, threats to transit systems, and other pertinent information. DOT and TSA began the process of establishing standards after the issuance of the Annex, but the effort has not produced any consensus standard yet. However, TSA projects that multiple consenus standards will be developed later in 2008.

TSA's best option for establishing an effective oversight program is to reengage in a consultative process to develop compliance

[5] Public Law 110-53 (2007)

standards, as required by the Annex.[6] DHS' oversight role in mass transit security is relatively new and much expertise in mass transit is concentrated in DOT and with mass transit system stakeholders. The American Public Transportation Association, a nonprofit organization whose membership includes most of the major mass transit rail system stakeholders, has a Project Management Team for Standards and Research. This is the logical forum for developing TSA's security standards, because it includes TSA, DOT, all Tier I mass transit systems, and state departments of transportation, as well as transit unions.

In addition, TSA needs to reconcile the assessment and compliance facets of the Surface Transportation Security Inspection Program. Assessments are essential, but TSA also has a mission to advance the security baseline. The BASE assessment's purpose includes identifying programs and protocols that might be effective models for other systems. Grant funding based on assessments would be an effective incentive to improve security, but compliance regulations based on assessments are needed as well.

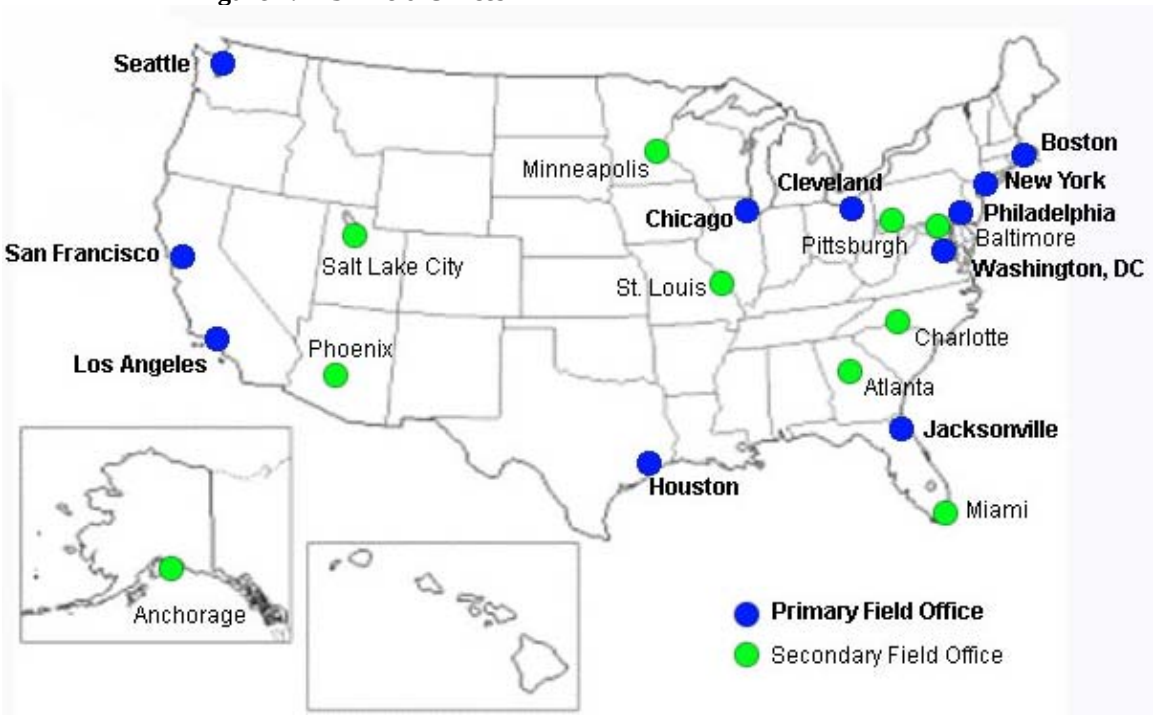
## Command Structure Inhibits TSI Effectiveness

Surface Transportation Security Inspector priorities are set by numerous entities that do not fall into the same chain of command. TSIs must respond to taskings from multiple federal security directors and multiple headquarters components, and these taskings frequently focus on divergent objectives. Because of their command structure, TSIs are pulled in multiple directions and find it difficult to complete long-term objectives in mass transit systems. TSA is not benefiting from or building on the institutional knowledge and expertise of the TSIs. Returning the program to direct headquarters supervision, as it was prior to December 2006, would enable TSA to manage the TSI program better.

TSA initially managed its TSIs from headquarters. TSIs are organized into 11 supervisory offices and 10 satellite offices in cities with large mass transit systems or heavy freight rail traffic (see Figure 4). These field offices previously reported directly to the Office of Security Operations' Compliance Program at TSA headquarters.

[6] Memorandum of Understanding Between the Department of Homeland Security and the Department of Transportation on Roles and Responsibilities Concerning Public Transportation Security, September 28, 2004; the Annex to the Memorandum of Understanding, September 9, 2005

**Figure 4: TSI Field Offices**



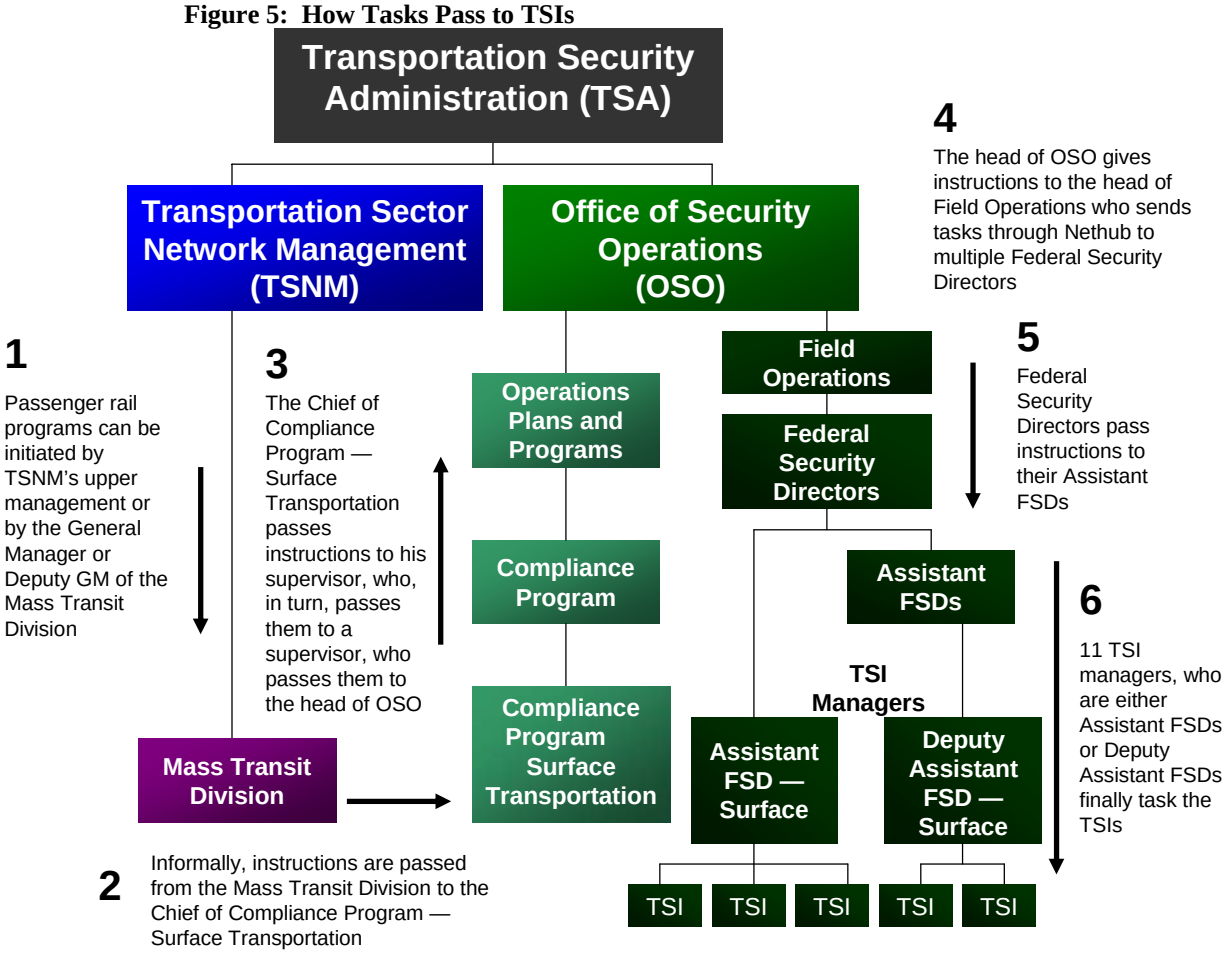

On December 20, 2006, TSA realigned each TSI – Surface field office under the authority of the federal security director at a local airport. Federal security directors are the highest-level TSA officials at an airport and provide operational leadership for transportation security responsibilities within an airport. The justification for this reorganization was to accommodate an increasing focus on hazardous material security issues, expanded compliance inspections, and outreach and liaison efforts with industry stakeholders to ensure that they understand and implement recommended security action items. However, this realignment left the Office of Security Operations' Compliance Program in charge of the Surface Transportation Inspection Program, just not in charge of the TSIs themselves.

Due to the realignment, TSIs can receive assignments from multiple sources including the Office of Security Operations' Compliance Program, the local federal security director, other federal security directors in the region, TSNM at headquarters, and, in the case of VIPR exercises, the Office of Law Enforcement. These assignments and taskings often reach the TSIs through circuitous routes.

For example, when TSNM initiates a new program or requirement, instructions pass informally to the section chief for Surface Transportation Security Inspections in the Office of Security

Operations' Compliance Program. The section chief then more formally makes a request to the director of the Office of Security Operations. The director tasks the federal security directors who supervise the supervisory TSIs in the field (see Figure 5). In practice, because the section chief holds weekly conference calls with the supervisory TSIs to discuss priorities and share information, the supervisory TSI often informs the federal security director about headquarters mandates. These individuals must work together to assign resources, which might fall in the administrative jurisdiction of another federal security director.

**Figure 5: How Tasks Pass to TSIs**




Federal security directors may also initiate assignments locally, meaning they are not nationally coordinated. In our survey, 65% of TSIs disagreed with the statement that their federal security directors and TSA headquarters officials coordinate well with each other. Only 30% believed they have sufficient direction and information from their chain of command to do their jobs effectively.

Although the goal of the December 2006 reorganization was to expand compliance inspections and liaison with industry stakeholders, in practice it is weakening TSA's expertise in mass transit rail security. TSA designated the 11 field supervisory TSIs as Assistant Supervisory Federal Security Directors for Surface Transportation and placed them under one of the local federal security directors at an airport in their primary city. Many TSIs said that TSA's decision compromised specialized rail experience and would ultimately undermine relationships that TSIs have built with mass transit rail stakeholders. Some TSA management officials at headquarters agreed with this assessment.

Many TSIs said that federal security directors have moved aviation inspectors without any rail experience into surface inspector positions. TSA officials also said that federal security directors have been hiring individuals who did not have sufficient relevant surface transportation experience for TSI positions. Some federal security directors assign TSIs to shifts in support positions in aviation, such as filling in for TSA screeners by observing exit lanes at airports. TSA hiring practices under the Surface Transportation Security Inspection Program were not part of our scope, and we did not assess the extent of under qualified and underutilized TSIs. However, such practices conflict with the requirement of the *9/11 Commission Act* that states TSIs should have "relevant transportation experience" and are to be used "to assist surface transportation carriers, operators,… and facilities to enhance their security."

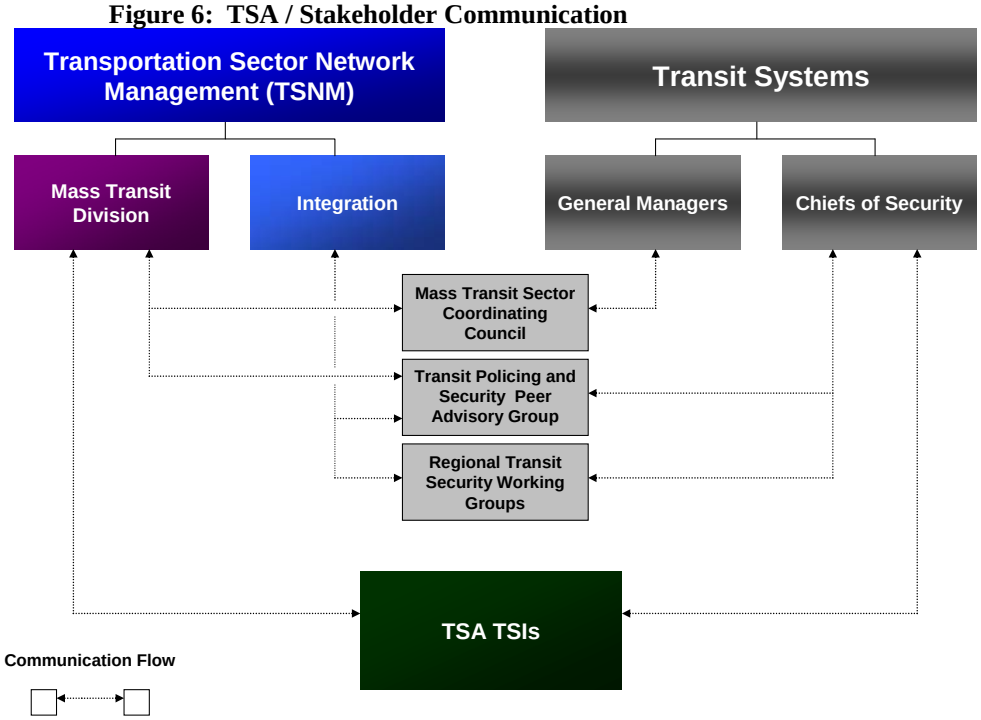
Most TSA officials involved in surface transportation say that the previous placement of the TSIs under direct headquarters supervision worked well. While many of the TSIs have high regard for their supervisory federal security director, only 4% said they preferred to retain the current chain of command. The remaining TSIs considered the optimal arrangement for their program to be a unified chain of command, with TSIs reporting to their current regional Supervisory TSIs, who would report to a headquarters component with authority over surface transportation. Many of the headquarters officials we interviewed also supported a dedicated headquarters surface transportation component overseeing the TSIs. Several TSA officials said that TSA headquarters successfully manages other field programs including the NEDCTP, the Federal Air Marshals, the Office of the Chief Counsel, and media relations.

## TSA Needs To Coordinate its Communication Efforts

TSA policymakers and TSIs both conduct substantial outreach with mass transit and passenger rail systems. However, policymakers do not consistently give sufficient information to TSIs, so mass transit officials do not view TSIs as a viable communication link to TSA headquarters. Furthermore, not all TSA policymakers have full access to TSI work products. TSNM and the TSI program should address these deficiencies that weaken what would otherwise be one of TSA's strengths in mass transit security.

Both TSNM and the Surface Transportation Security Inspection Program share responsibility for fostering communication with transit stakeholders. TSA's division for policy and coordination, TSNM, has several ongoing initiatives requiring communication with stakeholders. It has established forums, such as the Mass Transit Sector Coordinating Councils, where Mass Transit Division representatives meet with mass transit general managers to discuss rail security priorities. TSNM and DOT hold biannual Transit Safety and Security Roundtables with mass transit security chiefs to discuss initiatives such as training, public awareness campaigns, and emergency drills. TSNM Integration holds Regional Transit Security Working Groups to negotiate agreements on a region's Transit Security Grant applications. Additionally, TSNM Mass Transit Division holds a monthly Peer Advisory Group conference call with transit security chiefs, and periodic in-person conferences with the group to discuss mass transit programs (see Figure 6).

**Figure 6: TSA / Stakeholder Communication**




TSIs in the field also conduct thousands of hours of stakeholder outreach each year. Often, this occurs through less formal interactions than the TSNM communication. TSIs routinely hold personal meetings with mass transit officials and attend stakeholder conferences or events. Maintaining good working relationships with mass transit personnel is an essential part of a TSIs job, and many stakeholders view their local TSIs as the face of TSA.

Despite these efforts, the need for more coordination between TSNM at headquarters and the TSIs in the field has affected the flow of information to and from stakeholders. TSNM and TSIs share responsibility for stakeholder outreach, but TSIs said that TSNM does not always give them sufficient information about its policy initiatives and grant processes. Stakeholders expressed confusion on a number of TSA programs and guidelines, including the VIPR and grant program, but many said TSIs did not have enough helpful information. Many of the TSIs we interviewed agreed, saying that this situation limited their credibility with stakeholders.

According to several TSIs, TSNM has not always included them in local meetings between TSNM and mass transit agencies, specifically Regional Transit Security Working Groups and Peer Advisory Groups. Supervisory TSIs reported that their omission

from these forums affected their ability to advise and liaise with stakeholders. The reasons for these omissions were not clear.

In our survey, 29% of TSIs said that state officials and transit authorities perceive that there is cooperation and coordination between TSA headquarters and TSIs. When asked whether TSA headquarters personnel involve local TSIs in planning and holding meetings in their jurisdiction, 19% of TSIs said they had been included.

Additionally, information from TSIs is not always available to TSNM personnel. Although TSIs in the field regularly transmit their reports to TSA Headquarters, several TSNM employees involved in analyzing security threats and vulnerabilities said that they do not have direct access to TSIs BASE assessments, station profiles, and other reviews. This makes it difficult for TSNM to administer its security programs using a risk-management approach. The sensitive nature of these documents should not preclude TSNM employees from being able to use them.

Despite assurance given by TSA officials that individuals do have access to appropriate information and that TSIs are informed of meetings, we remain concerned that TSA is not fully leveraging its assets in the field, putting both TSIs and mass transit officials at a disadvantage. To serve as effective liaisons between TSA headquarters and mass transit agencies, TSIs should be aware of information TSNM is passing on to transit agencies. TSNM headquarters personnel and TSIs in the field need to improve internal communication, so that mass transit officials can consistently rely on TSIs as an information resource.

## Recommendations

We recommend that the Administrator of the Transportation Security Administration:

**Recommendation #1:** Place the Transportation Security Inspectors – Surface under the direct authority of a TSA headquarters official who is responsible for surface transportation, such as the Office of Security Operations' Assistant General Manager for Compliance.

**Recommendation #2:** Direct TSNM to provide TSIs information and updates on the rail-related programs. Invite TSIs to local meetings with stakeholders. Instruct the Office of Security

Operations' Compliance Program to make all TSI assessments and profiles available to employees of TSNM.

We recommend that the Assistant Administrator of the Office of Transportation Sector Network Management:

**Recommendation #3:** Develop specific, feasible security standards for mass transit systems. Incorporate applicable TSI assessments, and consult with DOT and relevant transit associations, such as the American Public Transportation Association, when developing these standards.

## Management Comments and OIG Analysis

TSA provided written comments on our draft report. We evaluated these comments and have made changes where we deemed appropriate. Below is a summary of TSA's written response to the report's first three recommendations and our analysis. A copy of TSA's complete response, with our general management comments, is included as Appendix B.

**TSA's Comments to Recommendation #1:**

TSA did not concur with the recommendation. TSA described the history of the Surface Transportation Security Inspection Program and summarized the current organizational structure of the program. TSA also described the various avenues for communication among all of the TSA components that interact with the TSIs at headquarters and in field offices. TSA stated that in December 2007 it reviewed the reporting structure of TSIs and had taken steps in recent weeks to "strengthen and clarify" TSI reporting lines, including "clearer definitions of roles and oversight responsibilities" of the program and the Federal Security Directors.

**OIG Analysis:** We are aware of TSA's December 2007 review. That review recommended that TSIs report directly to a headquarters official responsible for surface transportation. However, TSA never implemented this organizational structure. We maintain that the TSIs should be placed under direct headquarters supervision, at least until the program is more developed and field operations have been restructured to reflect the complexities of managing multiple transportation modes. Only four percent of the TSIs consider the current structure viable, and many of the headquarters officials we interviewed also support a

dedicated headquarters surface transportation component overseeing the TSIs.

It is not clear whether TSA has a viable alternative to address this issue. In its action plan, TSA should provide additional information describing how it has improved reporting lines.

This recommendation is Unresolved - Open.

**TSA's Comments to Recommendation #2:**

TSA concurred in part with the recommendation. TSA stated that it provided TSNM with "full and unfettered" access to the BASE assessments and station profiles, and had not denied a TSNM request for access to the assessments. However, TSA stated that within TSNM, access to the assessments is on a "need to know" basis to prevent negligent disclosure of sensitive information. It also reported that several methods exist that allow TSNM to provide TSIs with information and updates on the rail-related programs. Separately, TSA provided the names of individuals in TSNM who have "need to know" access to BASE assessments. TSA stated, "No [TSNM Integration] personnel have direct access to the BASE results reports and station profiles. As their duties warrant, TSNM Integration personnel may review these materials by coordinating with TSNM Mass Transit staff."

TSA provided an extensive description of methods for improving communication between TSIs and other TSA offices. Those methods include weekly or biweekly conference calls, annual briefings on grant guidance, TSI participation in grant panels, TSNM participation in STSIP meetings and annual national conferences, participation in a Mass Transit Security Information Network, daily headquarters communication, coordination between TSNM and the TSOC, and TSI participation in security standards meetings and in joint quarterly threat and analysis briefings. TSA concluded that TSNM Mass Transit "generally attempts to coordinate engagement with stakeholders through the TSIs," and provides examples of when such coordination occurred.

**OIG Analysis:** TSA's description of access to TSI assessments is partially responsive to our recommendation. However, we are concerned that TSNM Integration staff members, including the TSNM Integration General Manager, do not have direct access to TSI assessments. Our concerns stem from the fact that TSNM Integration officials negotiate directly with mass transit systems on grants, often without TSNM mass transit officials present. These

grants exceeded $300 million in FY 2008. We also remain concerned that TSNM only "generally attempts" to coordinate engagement with stakeholders through the TSIs. TSIs are the face of TSA for stakeholders, and failure to coordinate engagements through them to the fullest extent possible reflects less than desirably on TSA.

In its action plan, TSA should provide evidence of a policy memorandum or other guidance that demonstrates that TSI assessments are available to all TSNM staff involved in threat and intelligence assessments, and all senior TSNM Integration staff involved in the development of grants. The action plan should also describe a process for coordinating stakeholder communication more effectively; and provide a memorandum, policy guidance, or standard operating procedure documenting communication and notification requirements.

This recommendation is Resolved - Open.

**TSA's Comments to Recommendation #3:**

TSA did not concur with the recommendation. TSA stated that the recommendations to consult with DOT, APTA as well as other federal law enforcement and intelligence entities were already in practice.. TSA stated that it currently participates, along with the DOT Federal Transit Administration, in the APTA security standards development process that began in January 2006. TSA described in some detail the nature of its participation in this forum, and plans for additional initiatives. TSA also provided extensive comments on its cooperation with federal security partners and mass transit and passenger rail communities, and provided examples, such as the BASE reviews and Security Measures for Transit Tunnels that have increased the security baseline. TSA stated, "[because] these products reflect some of the most effective practices in the mass transit and passenger rail community, this effort is akin to standards development."

**OIG Analysis:** We applaud TSA's efforts in increasing the security baseline, but we disagree that voluntary compliance with security best practices is the same as mandatory compliance with security standards and regulations. The 9/11 Commission Act requires compliance inspections and enforcement of security regulations and directives, and TSA has not yet promulgated these regulations. Although we agree with TSA's observations about its accomplishments absent regulations, which are described in our

report, we identified areas in which regulations would make TSA more effective.

In its action plan, TSA should explain its progress toward developing security regulations and directives, as well as its collaboration with FTA and APTA.

This recommendation is Unresolved - Open.

## TSA and Mass Transit Authorities Are at Odds over Grant Program

TSA and stakeholders disagree on the best approach for allocating funds and prioritizing projects for the Transit Security Grant Program. As a result, TSA has made numerous changes to the grant award process, but has not yet developed a workable solution. These changes have frustrated stakeholders, who have raised numerous concerns about TSA's inconsistent and unpredictable processes, its negative effect on regional cooperation, and its inability to integrate asset-specific risk into its assessment methodology. Under the *9/11 Commission Act*, TSA is required to report how its grant awards address national transportation security goals, but TSA's current strategy of negotiated agreements may not provide sufficient documentation to evaluate the basis for TSA's grant decisions. A process for incorporating asset-specific risk assessments into grant decisions and a forum for stakeholders to evaluate whether TSA's grant strategy addresses their highest priority security needs, would enable TSA to develop a more objective and responsive grant process.

Until 2005, transit systems received security funding through the Department of Homeland Security's Urban Area Security Initiative grant program. Subsequently, the department established the Transit Security Grant Program to address the needs of transit systems (see Figure 7). TSA assumed responsibility for grant award decisions in the fiscal year 2006 grant cycle. In its first year of stewardship, TSA made grant award decisions through a competitive process. TSA initially allocated funds to a metropolitan region, based primarily on that region's ridership. Then each region's Regional Transit Security Working Group decided how much money each transit system would receive. Transit systems submitted as many as five Regional Working Group-endorsed grant requests to TSA. A panel that included officials from TSA TSNM, the Federal Emergency Management Agency (FEMA) National Preparedness Directorate, and DOT Federal Transit Administration then approved projects.

**Figure 7: DHS Grants for Mass Transit Systems, FY 2003-07**

| | FY 2003 | FY 2004 | FY 2005 | FY 2006 | FY 2007 |
|---|---|---|---|---|---|
| **Grant Program** | Urban Area Security Initiative Grant | Urban Area Security Initiative Grant | Transit Security Grant Program | Infrastructure Protection Program<br>Transit Security Grant Program | Infrastructure Protection Program<br>Transit Security Grant Program |
| **Amount (in millions)** | $65 | $50 | $150 | $143 | $171 + $100 supplemental |
| **Administrator** | Office of Domestic Preparedness | Office of Domestic Preparedness | Office of Domestic Preparedness | TSA | TSA |
| **State Involvement** | None, direct to Stakeholder | None, direct to Stakeholder | Yes, through State Administrative Agency | Yes, through State Administrative Agency | Yes, through State Administrative Agency |
| **Application** | Competitive applications | Competitive applications | Competitive applications | Competitive applications | Cooperative agreement |

Both TSA officials and stakeholders were displeased with the fiscal year 2006 grant cycle, but for different reasons. At the beginning of the fiscal year 2006 grant cycle, grant guidance allowed transit systems to fund projects that fell within one of six categories, including infrastructure and tunnel hardening, prevention and detection of nonconventional weapons, emergency drills, citizen awareness campaigns, employee training, and system-specific risk mitigation. After stakeholders submitted their fiscal year 2006 grant applications, TSA changed grant priorities to give the highest priority to training transit employees, and said the only remaining high priority category would be protection of underground and underwater tunnels. Stakeholders reported that, due to changed priorities, TSA denied projects that fell within the original application guidelines. Additionally, some partially completed projects from previous grant cycles were unfunded because of these changes.

Stakeholders expressed frustration that TSA's changing priorities made it difficult to plan security expenditures. Stakeholders also said that TSA set unreasonable deadlines for submitting proposals and that TSA's performance period of 36 months for spending awarded grant money was unrealistic, given rigorous and time-consuming state and city contract requirements. At the same time, stakeholders observed that TSA's grant award process was markedly slower and more cumbersome than other federal grant programs. At the time of our review, states were still awaiting decisions on fiscal year 2006 applications totaling almost $40 million. Some identified the need for an online application tracking process as a contributing factor.

TSA officials said that they were displeased with the fiscal year 2006 cycle because Regional Transit Security Working Groups did not allocate spending decisions based on risk, and project proposals did not address TSA's priorities. Instead, many Regional Transit Security Working Groups chose to divide funds so that most systems, regardless of size or risk, received at least one funded project. High-level TSA officials, including the Administrator and Deputy Administrator, became directly involved in communicating grant priorities and negotiating grant projects.

During 2006, TSA did not integrate asset-specific information into grant guidelines and priorities. Many state homeland security and transit security officials said that TSA's risk management approach did not account for differences in the infrastructures and needs of cities and their transit systems. For example, several transit officials said that TSA's decision to set journeyman training as the highest TSA priority overlooked extensive in-house training, which already met security needs. Some stakeholders said they had the impression that grant priorities were being set by political appointees, rather than by subject matter experts with knowledge of the region. Senior TSNM officials said that priorities were being set at a high level within DHS and were based on a preference for visible activities, such as training and security patrols.

For the 2007 grant cycle, TSNM developed a new approach to grant prioritization for Tier I systems, which officials refer to as a negotiated cooperative agreement. Previously, the Regional Working Groups for the Tier I regions delegated spending decisions to each individual transit system in the region. This year, TSA is working with the Regional Working Groups to identify the most significant risks in the region, and pool regional grant funding to address these risks in order of importance. TSA plans to make funding decisions based on negotiations with each Tier I regional working group, rather than setting general guidelines and relying on a federal panel or a peer review by transit security officials to grant awards based on eligibility.

Stakeholders are willing to try TSA's strategy of a negotiated cooperative award process, but concerns remain. The system still requires Regional Working Groups to submit proposals, both for the fiscal year 2007 grants and for a supplemental grant announced in August 2007. Deadlines for submitting supplemental proposals were initially two weeks. However, Tier I system managers complained that preparing a submission in two weeks was unreasonable. TSA responded to transit agency concerns by extending the deadline for Tier I systems to four months. Additionally, transit systems still did not have decisions on all fiscal year 2006 proposals to help plan their projects. Several stakeholders expressed frustration about being invited to submit proposals on any of seven TSA grant priorities, when TSA has denied applications that fell clearly within

the guidelines in the past (see Figure 8). Some state homeland security officials expressed frustration that TSA does not support investment in complex infrastructure-hardening projects, by not guaranteeing multiyear funding. Without the ability to plan for the long term, states will request funding for operational costs and off-the-shelf technologies such as closed-circuit television cameras, which may not mitigate as much risk as projects that are more ambitious.

**Figure 8: TSA Grant Priorities**

- Protection of high risk/high consequence underwater/underground assets and systems;
- Protection of other high risk/high consequence assets and systems that have been identified through system-wide risk assessments;
- Use of visible, unpredictable deterrence;
- Targeted counter-terrorism training for key front-line staff;
- Emergency preparedness drills and exercises;
- Public awareness and preparedness campaigns; and
- Efforts in support of the national preparedness architecture (regional collaboration and communication, response plans).

Many stakeholders had reservations about TSA's plans to determine regional funding priorities through stakeholder consensus. They envisioned that the large transit agencies in a region would receive most, if not all, of the grant money, and smaller agencies would receive nothing. Many of the bigger transit agencies would rather forgo a larger share of TSA funding in order to preserve good relationships with their smaller regional partners. Several officials commented that the relatively small pool of grant money was not worth the cost of resentment from the small transit systems. Most regional homeland security officials said that because they receive funding from several DHS grant programs, from DOT, and from state sources, they could reallocate other resources to restore balance among mass transit systems and fund their own highest priorities, essentially nullifying the effect of TSA's cooperative system.

Stakeholders expressed skepticism regarding TSA's commitment to establishing truly consensus-driven risk and funding priorities. In some regions stakeholders said that TSA has tried to negotiate separately with larger transit systems in the region, rather than working solely through the Regional Transit Security Working Group. Some stakeholders fear that cooperative agreements will enable TSA to control the Regional Working Group and ignore regional priorities.

Although cooperative agreements may aid TSA in learning about the asset-specific needs of stakeholders, the grant process still needs to incorporate asset-specific assessments of risk, as required by the Transportation Sector-Specific Plan. The Plan requires TSA to evaluate threats, vulnerabilities, and consequences against each asset and develop

countermeasures at the asset level. These assessments are needed to verify the concerns of stakeholders and substantiate the priorities of TSA.

TSIs can provide asset-specific information for the grants program. They conduct formal assessments of mass transit rail systems, have access to vulnerability and risk assessments conducted by mass transit systems, and develop considerable asset-specific information through routine consultation. Their contribution could verify the determinations of stakeholders and provide transparent substantiation for TSA decisions. However, TSA does not systematically incorporate this information into its grant assessment or prioritization process.

In addition, the fiscal year 2007 process may not generate an adequate written record of how grants were prioritized and awarded. TSA will decide grants for Tier I regional working groups through high-level negotiations with stakeholders. The TSA negotiators will not be operating from the same system-specific risk assessments as the regional working group members who participate in the negotiations. Awards may not be based on objective grant eligibility criteria. In these circumstances, there is a possibility that decisions might be personality-driven, that negotiations will be protracted, or that they will stalemate.

Without objective criteria for grant awards or a transparent process, it will be difficult for an outside observer to determine how and why TSA and the regional working group reached a decision. While we do not recommend that TSA disrupt its current grant cycle, TSA should use all of the risk information it has available, including information gathered by TSIs, to develop grant eligibility criteria and to enhance grant decision-making. The grant process should accommodate asset-specific grant priorities that recognize differences in vulnerabilities by region and transit system. It should also be sufficiently transparent that an independent observer can verify how TSA officials made grant decisions that were negotiated directly with regional working groups.

## Recommendations

We recommend that the Administrator of the Transportation Security Administration:

**Recommendation #4:** Develop procedures for incorporating asset-specific risk and vulnerability assessments, including information provided by TSIs, into the grant decision-making process and grant guidance. Designate a TSI from each major field office to provide updates to TSNM on the status of grant projects.

**Recommendation #5:** In TSA's annual report to Congress on how it used grants to implement its transportation security goals, TSA should include each grant recipient's assessment of the grant application and award process.

## Management Comments and OIG Analysis

**TSA's Comments to Recommendation #4**:

TSA concurred with the recommendation. TSA reported that it was using asset-specific security assessments, including information provided by TSIs, in the grant decision-making process and grant guidance. TSA also agreed that use of the TSIs to provide grant oversight would be a key component of the overall approach to mass transit security. TSA stated that TSNM and OSO were working together to develop a plan for this new TSI activity.

**OIG Analysis:** We consider these actions responsive to our recommendation. In its action plan, TSA should provide documentation verifying the incorporation of asset-specific assessments into the grant process, and a draft plan for the use of TSI's to verify grant oversight.

This recommendation is Resolved - Open.

**TSA's Comments to Recommendation #5**:

TSA concurred in part with this recommendation. TSA stated that including assessments from every eligible mass transit agency would "prove unduly time-consuming and burdensome." TSA proposed providing Congress a summary of applicant feedback with pros and cons.

**OIG Analysis:** We encourage TSA to provide a summary of applicant feedback, analysis or any additional relevant documents with its annual report to Congress. However, each grant recipient's assessment of the grant application and award process should also be included. TSA should provide our office with a copy of its first annual report to Congress, when it becomes available.

This recommendation is Resolved - Open.

## TSA Has Experienced Mixed Results with its Security Asset Deployments

TSA provides security assistance to mass transit systems through two programs: the VIPR teams and the National Explosives Detection Canine Teams. TSA's initial VIPR deployments would have benefitted from more precise planning, better consultation, and more use of local expertise and knowledge. The initial exercises occupied local law enforcement resources and strained relations with state and local homeland security officials. TSA has taken appreciable measures to strengthen coordination and protect the identity of participating federal air marshals. TSA should develop Memorandums of Agreement with individual mass transit systems to enhance VIPR's effectiveness.

Participants in TSA's NEDCTP consider the program well run and responsive, and approve of TSA's training and the quality of TSA dogs. TSA may increase participation in the program by considering alternatives to its requirement that handlers attend a 10-week training course in Texas, and by assisting smaller agencies, which do not have existing canine programs, to cover extensive start-up costs.

### The Visible Intermodal Prevention and Response Program

The VIPR Program experienced numerous problems during its early deployments. During the July 4, 2007 holiday week, TSA headquarters launched simultaneous VIPR exercises in New York, Boston, San Francisco, Chicago, Washington, DC and several other major mass transit cities. According to almost everyone we interviewed, TSA did not effectively communicate the timing, procedures, and rationale of the deployments with its own personnel or transit authorities. As a result, most of the early deployments generated controversy among TSA field offices, state homeland security officials, and mass transit officials. TSA has since addressed many of these concerns, but mass transit agencies would be more willing participants in the program if they had system-specific agreements with TSA.

### Issues with Early VIPR Deployments

*TSA gave little warning to its field personnel and mass transit stakeholders.* For the July 4 holiday deployments, TSA field officials received notice of the exercise on the weekend before the holiday, and many said they were embarrassed to ask the transit systems to accommodate the VIPR directive on such short notice. Tensions developed between some federal security directors and federal air marshal special agents in charge over which TSA

official had the lead. When asked why TSA deployed VIPR teams on short notice, several TSA officials said that they were testing the emergency response capabilities of TSA field officials. This strategy is disruptive to local transit police, who plan months in advance for major holidays and events, and in an emergency rely on backup from metropolitan police.

*TSA field officials said the initial exercises put their safety at risk.* TSA required federal air marshals to wear raid jackets or shirts identifying them as air marshals, which potentially compromised their anonymity. In response to this concern, TSA changed the policy; federal air marshals now attend VIPR exercises in civilian clothes or jackets that simply identify them as DHS officials. Many TSIs also questioned TSA's decision to place civilians in TSA raid jackets on the systems, because TSIs are unarmed and might become a target if mistaken for federal law enforcement officers. TSA screeners and behavioral detection officers deployed on VIPR teams face the same concern.

*The initial VIPR deployments caused logistical and operational problems for state and local homeland security officials and mass transit security officials.* Many TSA employees on the VIPR teams had little or no experience on the transit systems on which they were deployed, and none had a prearranged means of communicating with transit security officers. Because most TSA employees did not have system-specific training and means of communication, local transit police had to reassign officers to accompany VIPR teams, who were sometimes confined to areas outside the transit rail systems, such as in adjacent parking lots. In many systems, a transit police officer was assigned to each TSA employee, both to provide a means of communication, and to respond if the TSA employee observed anything suspicious or interacted with a passenger. Assigning transit police to accompany TSA employees cost transit systems increased overtime expenses, which TSA did not reimburse.

*Federal air marshals were unfamiliar with local procedures and concerns.* Some transit security officials reported that federal air marshals were unfamiliar with local laws, local police procedures, the range of behavior encountered on public transportation, and the parameters of their authority as federal law enforcement officers. In several cities, the VIPR deployments caused tensions between transit officials and police unions. Some police unions interpreted the introduction of VIPRs as replacing union transit police officers, or saw the TSA presence as an acknowledgement that the system

was hiring insufficient transit police to address genuine security needs.

*TSA headquarters, TSA field officials, and mass transit security officials disagreed over the placement and composition of the VIPR teams.* TSA instructed its local officials to patrol designated stations, which conflicted with local strategies on police visibility and coverage. In one city, TSA chose lightly traveled stations although the transit police wanted them in the city center; in two other cities, TSA chose the largest stations in the system, which already had a heavy police presence. Some transit security authorities refused to accept the full complement of 42 TSA employees envisioned in the VIPR deployments, or refused to allow them into the transit systems.

*VIPR planning did not include sufficient local participation.* TSA field officials and transit security officials said that the quality of TSA headquarters' Concept of Operations, and its strategy of deploying VIPR teams without sufficient stakeholder consultation, demonstrated operational inexperience. Many TSA and transit system officials said that TSA did not have an effective feedback process to evaluate programmatic weaknesses. Though local TSA officials had a better understanding of the local environment, headquarters planned most of the exercises without participation from the field.

*Participants and outside observers questioned the value of VIPR exercises.* In a July 11, 2007, letter to the Secretary of the Department of Homeland Security, the National President of the Federal Law Enforcement Officers Association described the VIPR exercises as "clearly a waste of scarce Federal Air Marshal resources." TSIs also considered their participation in VIPR exercises unproductive. In our survey, we asked the TSIs to select the two duties they performed that they considered the least effective use of their time, and 70% selected VIPR exercises as one of the two. In their current configuration, for which the only visible TSA presence during VIPR exercises is unarmed TSIs and aviation screeners in raid jackets, VIPR teams may be less valuable to transit police than funding overtime pay for their officers.

## Improving the VIPR Program

TSA headquarters officials responsible for the VIPR program were aware of criticisms of the July 4 holiday deployments, and developed an internal consultative process to restructure the VIPR program. They set up a Joint Coordination Center to facilitate

stakeholder communication and improve the scheduling of exercises. In September 2007, TSA convened a meeting of VIPR Joint Coordination Center personnel, TSNM Mass Transit personnel, Federal Air Marshals, TSIs, and mass transit security chiefs. This meeting resulted in the creation of mutually agreed upon nationwide operating guidelines for the VIPR program. TSA officials also improved stakeholder communication by giving presentations to mass transit security chiefs and providing better guidance to TSA field personnel about the objectives, execution, and resources of the VIPR program.

In response to comments made by TSA officials during our exit conference in February 2008, we had follow-up discussions with TSA officials and stakeholders about the evolving nature of the VIPR program. TSA officials said that VIPR exercises are now voluntary and emphasized that transit systems may refuse to participate in any given deployment without losing eligibility for grant funding or future operational assistance. Local transit officials now decide where TSA will deploy VIPR teams and which elements of the VIPR model TSA will include. For example, transit officials could opt for just federal air marshals patrolling in plainclothes with local police, or just TSIs assisting local police with screening checkpoints. In most regions, transit officials now have a local TSA point of contact that will help plan and coordinate the exercises, and answer stakeholder questions. Some systems are now comfortable allowing experienced VIPR teams to patrol without the accompaniment of local transit police. Transit officials also confirmed that TSA is providing two weeks notice when it wishes to conduct an exercise, instead of the three to seven day notice that it gave in July and August 2007. This lengthened notification period is an acceptable compromise for many of the stakeholders.

Despite these improvements, TSA needs to address some remaining system-specific coordination issues. Because of the problems encountered during the July 4 deployments, several mass transit security chiefs stated that they would not consider using VIPR teams in the future without a written agreement between their transit agency and TSA. TSA has a nationwide Concept of Operations document that contains general guidelines on the planning and execution of a VIPR deployment, and TSA works with participating stakeholders to develop detailed written operation plans for each specific VIPR deployment. However, TSA does not have written VIPR-related agreements with any major mass transit systems. TSA and a specific mass transit agency could structure these agreements to ease the stakeholder's

concerns – such as training requirements, communication systems, and law enforcement authority – while still enabling VIPR deployments to be agile and unpredictable.

The *9/11 Commission Act* authorizes TSA to deploy VIPR teams, but it requires TSA to consult with local security and law enforcement officials to develop and agree upon appropriate operational plans, and provide relevant information before and during the deployment. Most mass transit system security officials welcome some form of TSA operational assistance, when that assistance is well planned and appropriate to local political conditions. While TSA has made progress in addressing the problems with early VIPR deployments, it still needs to develop a more formal collaborative relationship with local transit officials if its VIPR exercises are to enhance mass transit security.

## The National Explosives Detection Canine Team Program

Stakeholders support TSA's recent adaption of the NEDCTP to the rail environment. TSA provides participating mass transit agencies with a free canine and a $40,000 annual stipend for each handler. By absorbing a significant portion of the cost of each team, the program allows the transit agencies to direct financial resources toward other needs. Several agencies recognize the importance of TSA's annual certification standards, because they help ensure that the dogs continue to perform. Agencies also appreciate that TSA recently modified the training facility and program to meet the needs of participants better. For example, TSA recently built a mock rail station and began offering short "executive courses" that were directed at the handlers' commanding officers.

Most stakeholders consider TSA's training program excellent, but view the requirement to send officers to a ten-week training course in Texas as burdensome. Transit agencies have to pay overtime to backfill for the officer who is at training, which could create a financial liability for some transit agencies. Experienced canine handlers who participate in the program are required to attend for the full ten weeks, even though they already possess many of the skills that the training teaches. Furthermore, the most qualified officers selected as handler candidates are not always willing to leave their homes and families for such an extended period. While most transit agencies look past these issues, we did learn of two agencies that do not participate in the program for this reason.

The certification and recertification process for TSA canines is very strict, and can sometimes cause coordination problems

between TSA and local canine teams. There is no single national standard for explosive detecting canines; individual federal and state programs decide which standards, if any, they will use. In states without standards, many transit agencies praise the TSA program because a TSA canine's performance is independently verifiable while a local canine's performance is not. However, in states with existing explosive detection standards, TSA standards may conflict with local standards. This complicates integrated training exercises with both TSA canines and transit agency canines because teams may have to train differently. Again, most transit agencies are willing to work through these issues, but national, verifiable standards for canine explosive detection teams would alleviate some of these problems.

Small transit agencies without existing canine programs face extensive additional start-up costs. TSA covers the cost of acquiring the canine and training the team, and provides a $40,000 stipend. However, when beginning a program, an agency must also spend money on its first kennels, canine-ready vehicles, and secure containers for storing explosive training materials. In systems that receive several canines, these costs can be as much as $300,000. Most transit agencies that participate in the TSA program are large agencies that had a pre-existing explosive detection program, and therefore had already invested in these start-up capital expenditures. However, agencies with limited resources might elect not to join TSA's program because of the additional start-up expenditures. As TSA expands the NEDCTP, it should provide additional start-up grant funds for agencies without existing canine explosive detection units.

The *9/11 Commission Act* states that TSA should develop a certification program for non-TSA explosive dogs, and encourages TSA to explore ways to expand its canine explosive detection units. Transit systems that participate in the program are pleased with the canines they receive and with TSA's ongoing certification program. Any measures TSA can take to make this program more widely available would contribute to mass transit rail security.

## Recommendations

We recommend that the Administrator of the Transportation Security Administration:

**Recommendation #6:** Seek Memorandums of Agreement with all relevant transit authorities regarding VIPR deployments. These

Memorandums of Agreement should: describe a Concept of Operations or Standard Operating Procedure for both planned and unforeseen events; explain how TSA personnel will communicate with transit authorities and other local law enforcement; and identify the legal authorities that VIPR team members will have in the event of an emergency. The Memorandums of Agreement should specify that participation in VIPR exercises is voluntary and at the request of the local transit authority.

**Recommendation #7:** Revise grant program eligibility criteria to allow start-up funds for mass transit systems that do not already have a canine explosive detection unit.

## Management Comments and OIG Analysis

**TSA's Comments to Recommendation #6:**

TSA concurred in part with this recommendation. TSA agreed that much of the requested information set forth in this recommendation was valuable, which was why the information was included in the nationwide concept of operations document and the individual operations plans that were written before each VIPR deployment. TSA also stated that a formal Memorandum of Agreement for each individual VIPR deployment would hinder VIPR performance and diminish the overall effectiveness of the program. TSA did not agree with our recommendation that the Memorandum should specify that the local transit authority should initiate VIPRs. TSA asserted that there was no legal requirement for VIPRs to be stakeholder driven, and such a requirement would limit TSA's options.

TSA stated that the remainder of the material that we recommended be codified in a memorandum is already part of the VIPR planning and deployment process, and specifically included in the concept of operations document. TSA stated that it also disseminated information to TSA field personnel and mass transit stakeholders about the planning and conduct of VIPR operations.

**OIG Analysis:** We consider these actions partially responsive to the intent of the recommendation, but maintain that TSA should enter into a written agreement with each transit agency that hosts VIPR deployments. This would give mass transit agencies confidence that their concerns have been formally addressed.

We are not suggesting that TSA must develop a Memorandum of Agreement for each individual VIPR deployment. As TSA pointed out, such a requirement would be an unnecessary administrative burden. We also concur that a one-size-fits-all approach is neither advisable nor effective. The VIPR concept of operations document, however, is a one-size-fits-all document; it applies to all VIPR exercises and all mass transit agencies. Conversely, the individual operations plans are detailed, specific descriptions of how a VIPR team will conduct a single deployment, and they do not contain high-level information about the nature of VIPR on that transit system. Both of these documents are useful, but neither provides a description of how VIPR deployments, in general, will be conducted within a specific mass transit agency.

Our recommendation aims to address this gap by suggesting TSA and transit systems create a formal agreement that defines VIPR in that system. Some major mass transit systems will not permit VIPR exercises on their premises because they believe there are important, unresolved legal issues. In addition, without formal acknowledgement that VIPRs are voluntary, we share stakeholder concerns that VIPR deployments might once again be conducted without stakeholder consent or advanced notification Even when intelligence indicates heightened threat on a particular system, TSA should approach the transit authority and let them decide whether a VIPR deployment is warranted.

In its action plan, TSA should provide additional information that demonstrates it has given individual mass transit systems the option of a written agreement governing VIPR operations.

This recommendation is Unesolved - Open.

**TSA's Comments to Recommendation #7:**

TSA concurred with our recommendation. The Transit Security Grant Program allows eligible mass transit agencies to apply for $150,000 per team per year for start-up and sustainment costs. Agencies that train and certify under the NECDTP are not eligible to receive this grant funding. However, agencies participating in the NECDTP do receive $40,000 per team per year to cover sustainment costs.

**OIG Analysis:** We consider these actions partially responsive to our recommendation. TSA did not provide details of its future plans. We are recommending that transit agencies without existing canine programs, including those agencies that participate in the

NECDTP, be eligible for grant funds to cover some of their start-up costs. We do not expect that every participating agency will need supplemental start-up funds, but it is important that participation in the NECDTP does not exclude agencies from requesting necessary funds.

In its action plan, TSA should provide revised grant guidance that allows new participants in the NECDTP to apply for start-up funds for their program.

This recommendation is Resolved - Open.

The purpose of our review was to evaluate TSA's four largest oversight and assistance programs for mass transit rail: the Surface Transportation Security Inspection Program, the Transit Security Grant Program, the Visible Intermodal Prevention and Response program, and the National Explosives Detection Canine Team Program. Our goal was to evaluate how well TSA managed these programs and how well the programs met the security needs of the major mass transit rail systems.

The *9/11 Commission Act*, which was enacted shortly after we began our review, introduced new mass transit rail standards and responsibilities for TSA. Where we obtained information on the current status of TSA compliance with standards introduced by the *9/11 Commission Act*, we have included it in our report.

The scope of this review is limited to the four TSA programs listed above. The review does not encompass TSA's responsibilities for freight rail and for intercity passenger rail, or for other forms of mass transit, such as buses. The review therefore does not reflect the full range of responsibilities of the TSA officials who manage mass transit rail programs. We did not review TSA's strategic and long-term rail security initiatives, such as refining TSA's approach to risk management, developing TSA's intelligence sources and analysis, or identifying rail-specific research and development technology projects. Our conclusions about TSA's administrative and management challenges should not be generalized to include any of these programmatic areas.

We conducted our fieldwork from June 2007 to October 2007. While we recognized that each of the four programs under review was developed and implemented on short timelines and represented a significant new contribution to mass transit rail security, our review focused on the current status of the four programs. In the case of the VIPR program, TSA introduced major changes to the program after the period of our review. Therefore, we followed up with appropriate program officials and incorporated the result of those discussions in our report.

During the period from June 2007 to October 2007, we interviewed more than 100 individuals involved in the security of the nation's passenger rail system. We interviewed representatives from TSA's Office of Transportation Sector Network Management, Office of Law Enforcement, and Office of Field Operations. We also interviewed federal air marshals, transportation security officers, canine program coordinators, and

federal security directors. We spoke with more than one-fourth of the 88 TSIs. Using a website, we also surveyed TSIs on the various aspects of the Surface Transportation Security Inspection Program. Of the 88 current TSIs who received the survey, 83 replied. Survey respondents could remain anonymous, but many identified themselves and volunteered for follow-up telephone interviews. We also spoke with officials from DOT Federal Transit Administration, DOT Federal Railroad Administration, DOT Office of Inspector General, DHS Science and Technology, DHS National Preparedness Directorate, FEMA National Preparedness Directorate, and the Government Accountability Office.

We spoke with officially designated TSA primary or alternate security coordinators for the mass transit systems under review, as well as other officials responsible for security and grants coordination. The systems reviewed account for 85% of all passenger rail ridership in the United States. These included the systems listed below:

- New York Metropolitan Transit Administration (MTA),
- Port Authority Trans-Hudson (PATH),
- Washington Metropolitan Area Transportation Authority (WMATA),
- Chicago Transit Authority (CTA),
- Northeast Illinois Regional Commuter Railroad Corporation (Metra),
- Massachusetts Bay Transportation Authority (MBTA),
- Bay Area Rapid Transit (BART),
- San Francisco Municipal Transportation Agency (Muni),
- San Mateo County Transportation Authority (Caltrain), and
- Metropolitan Transit Authority of Harris County, Texas.

We also interviewed state homeland security officials for the regions with major mass transit systems, to discuss both the grant process and their overall relationship with TSA on mass transit rail security.

We also interviewed representatives from national transit stakeholder entities including Amtrak Office of Inspector General, the American Public Transportation Association, the Association of American Railroads, and the Amalgamated Transit Union.

In addition to testimonial evidence from interviews with subject matter experts, we requested and reviewed documentation from

TSA, as well as documentation provided by our interview subjects and obtained from public sources. This documentation includes:

- Laws, regulations, security directives, and court decisions relevant to mass transit rail, and federal authorities and responsibilities
- Public comments to the Notice of Proposed Rulemaking on Rail Transportation Security, 49 CFR Parts 1520 and 1580
- Memorandums of Understanding between TSA and the Department of Transportation, and relevant Annexes
- Memorandums and organizational charts documenting reorganizations and personnel changes within TSA
- Budget documents for TSA programs under review
- TSNM Integration grant information, including lists of stakeholder outreach communications and meetings, project proposals submitted by Tier I stakeholders, grant guidance and grant application kits, an overview on the use of cooperative agreements, documentation of grant decisions made by review panels, and grant allocation and dispersal timelines
- Documentation on the VIPR program, including citations to the arrest authority of Federal Air Marshals, policy memorandums and planning documents, concept of operations documents, and lists of VIPR deployments on mass transit rail
- Documentation on the TSA canine program
- Classified material generated by TSA related to mass transit rail security
- Training materials developed for an introductory rail course for Federal Security Directors
- Training materials and guidance developed for TSIs, including operational guidance, standard operating procedures, legal authorities, historical context, technologies, and duties and responsibilities of federal employees
- Sample BASE assessments, Station Profiles, Toxic Inhalation Hazards assessments, and other assessment tools, including their underlying legal authorities, operational guidance, and worksheets
- Sample weekly status reports on the activities of TSIs, including stakeholder liaison meetings, assessment site visits, trainings attended and provided, liaison with State Safety Oversight Agency inspectors and Department of Transportation rail inspectors

- Memorandums, letters, and other documentation provided to the Office of Inspector General by TSA employees, law enforcement officers, organizations and associations involved in mass transit at the national level, and state and mass transit officials

This review was conducted under the authority of the Inspector General Act of 1978, as amended, and according to the Quality Standards for Inspections, issued by the President's Council of Integrity and Efficiency.

TSA provided extensive comments on its overall impressions of the report as well as specific responses to each recommendation. TSA concurred with and has already taken steps to address many of the issues raised in our report. However, TSA perceived that our scope was too narrow; that we did not grasp the enormity of TSA's program or give enough credit to TSA; and that we made overly broad conclusions about TSA's transit security strategy. TSA asserted that the report did not provide sufficient historical context or recognize recent and prior achievements; did not account for the multi-faceted means by which policymakers communicate with transportation security inspectors; and that we erroneously extrapolated issues to reach broad conclusions about the agency's entire mass transit security portfolio.

TSA appears to have misunderstood our scope, and therefore, misinterpreted many of our conclusions. Our scope was limited to evaluating four oversight and assistance programs, yet TSA attempted to highlight gaps between conclusions about those programs and the full breadth of its mass transit security initiatives. Our goal was to evaluate how well TSA managed these programs and how well the programs met the security needs of the major mass transit rail systems. Our report identified areas of TSA responsibility that we deliberately did not include in this review—such as freight rail, intercity passenger rail, or buses—and noted that our conclusions did not reflect the full range of responsibilities of the TSA officials who manage mass transit rail programs. Furthermore, the report cautions that our conclusions about TSA's administrative and management challenges should not be generalized to include any of these programmatic areas. In light of such scope limitations, we did not make broad judgments on the effectiveness of the administration and coordination of the entire mass transit and passenger rail security program, as TSA suggests.

TSA asserted that the report focused exclusively on a four-month period. The bulk of our fieldwork occurred from July 2007 to October 2007 but our research was not limited to this timeframe. In fact, that research plus dialogue with TSA officials who provided additional information about TSA's recent progress, led to many revisions to our draft report.

TSA also commented that our report did not address changes made since the Government Accountability Office's September 2005 report. We did not focus on whether TSA implemented the Government Accountability Office's recommendations because, prior to the start of our review, the Government Accountability

Office initiated a comprehensive follow up review. We coordinated with the Government Accountability Office to avoid redundancy.

Whether TSA is engaging or communicating with mass transit and passenger rail agencies was never in question during our review. We applaud TSA for the sheer volume of its stakeholder outreach. However, although informative, TSA's discussion of how headquarters personnel communicate with its inspectors did not eliminate our concerns about the effectiveness of these efforts. It is not clear whether TSA management fully understands how the inspectors see this issue and whether it has sufficiently addressed this matter. As recently as May 2008, we received reports of inadequate communication from TSA headquarters personnel to TSIs in the field.

We reported that only 29% of TSIs said that state officials and transit authorities perceive that there is cooperation and coordination between TSA headquarters and TSIs. When asked whether TSA headquarters personnel included local TSIs in planning and holding meetings in their jurisdiction, only 19% of TSIs agreed.

TSA also stated that the report failed to address progress in the VIPR program. In fact, the report specifically addresses how TSA has improved the VIPR program over the past year, and describes many of the "lessons learned" from the July 2007 deployments. For several of the transit agencies that we spoke with, the July 2007 deployments were their first interaction with the VIPR program, and the size and number of the deployments was unprecedented. For this reason, we closely examined the July 2007 deployments and the problems that occurred.

We focused on the status of these programs and as a result, identified concerns regarding chain of command, unclear missions, and insufficient communication. Although these are TSA's four largest oversight and assistance mass transit programs, we did not portray these concerns as systemic. We did not intend to downplay what the programs have accomplished, but instead identify challenges that exist in their execution. Despite TSA's progress as a whole, these issues are undermining agency efforts to advance mass transit security.

The following is TSA's written response to our report.

*Office of the Assistant Secretary*

**U.S. Department of Homeland Security**
601 South 12th Street
Arlington, VA 22202-4220

Transportation
Security
Administration

INFORMATION

MEMORANDUM FOR: Richard L. Skinner
Inspector General
Department of Homeland Security (DHS)

FROM: Kip Hawley KH
Assistant Secretary
Transportation Security Administration

SUBJECT: Transportation Security Administration (TSA) Draft Report
U.S Department of Homeland Security (DHS)
Office of the Inspector General (OIG) Draft Report OIG-07-XX,
"TSA's Administration and Coordination of Mass Transit Security Programs," February 2008

Purpose

This memorandum provides TSA's response to the OIG report entitled, "Transportation Security Administration's Administration and Coordination of Mass Transit Security Programs," to be printed with the final report. It provides a detailed summary of security programs initiated by TSA for mass transit and passenger rail systems. While TSA concurs with and has already taken steps to address many of the issues raised in the OIG report, TSA believes the report fundamentally misses the point on what is effective security in the mass transit environment. Simply put, TSA's security mission is driven by intelligence relating to terrorist risk and the best way to address the security issue is through a series of linked, layered, flexible, jointly delivered, unpredictable, measures—not just a focus on regulatory enforcement and study of a static environment. The detailed summary provided by TSA provides specific factual responses to the report, but there is a disconnect between the assumptions of the investigating team and the full picture of TSA's transit security strategy.

Background

For a 4-month period from June to October 2007, DHS OIG evaluated TSA's security oversight and assistance programs for mass transit and passenger rail systems, including TSA's Surface Transportation Security Inspection Program (STSIP), the Transit Security Grant Program, the Visible Intermodal Prevention and Response program (VIPR), and the National Explosives Detection Canine Team Program (NEDCTP). The Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act), enacted shortly after OIG began its review, required the DHS OIG to report to Congress on the performance and effectiveness of Transportation Security Inspectors (TSIs).

During its review, OIG interviewed personnel in TSA's Offices of Transportation Sector Network Management (TSNM), Law Enforcement, Field Operations, and Security Operations. OIG also spoke with officials from the U.S. Department of Transportation, DHS, and chiefs and directors of security and grant coordinators for a number of mass transit agencies.

At the conclusion of its review, OIG found that, with the exception of TSA's canine program, each of the programs reviewed has an unclear or unduly complex chain of command; an unclear mission or insufficient guidance; and insufficient communication.

The OIG report focused exclusively on a compressed 4-month period of time which failed to provide a historic context within which the public could more fully assess the achievements that have been made in recent years in mass transit and rail security. Isolated criticism, without an historic context providing the full scope and quality of TSA's efforts, is neither fair nor constructive. TSA believes that the OIG failed to consult relevant work completed in this area by the Government Accountability Office (GAO) and used a narrowly focused review to reach broad conclusions about the agency's mass transit security programs.

GAO completed a comprehensive audit of TSA's passenger rail security programs in 2005. Since that time, TSA has provided progress reports on its efforts to implement the GAO recommendations. If the OIG had reviewed the 2005 GAO report and TSA's documented track record in implementing the GAO recommendations, the OIG would have been afforded a wealth of data for comparison of the mass transit security program's current state and to track developments, improvements, and continuing difficulties. However, in conducting its inspection, OIG did not request or consult these materials to assess progress in TSA's mass transit and passenger rail security program since September 2005. Instead, the report presents a snapshot, apparently based in substantial part on anecdotal complaints that are presented as the norm when in fact they are the exception.

Discussion

While the objectives of this audit were ostensibly to focus attention on management of just four components of the TSA's mass transit and passenger rail security program – STSIP, Transit Security Grant Program, VIPR Teams, and NEDCTP – the conclusions and recommendations are stated more broadly as judgments on the effectiveness of the administration and coordination of the entire mass transit and passenger rail security program.

In multiple areas, the report's analysis, conclusions, and recommendations reflect an incomplete understanding of the mass transit and passenger rail security program. Repeatedly, security programs are described as suffering from poor coordination, management, and administration when in fact extensive efforts in these areas have been undertaken or are ongoing.

**The Report Significantly Understates the Achievements of the STSIP.**

In its discussion of the STSIP, the report states that due to lack of "comprehensive security regulations" for mass transit, TSIs are hindered in their ability to carry out their mission and provide formal oversight of mass transit rail. Promulgation of the regulations mandated by the 9/11 Commission Act will expand the means available to TSIs in their security oversight and

inspection activities. However, the report's failure to discuss even in summary form the multiple and varied means by which TSIs have engaged mass transit and passenger rail agencies to advance strategic priorities – all accomplished without regulations – conveys the inaccurate and unfair impression the STSIP has not been effective.

*Baseline Assessment for Security Enhancement Program*

In partnership with the Federal Transit Administration (FTA) and the mass transit and passenger rail community, TSA developed and implemented the Baseline Assessment for Security Enhancement (BASE) program. The BASE program aims to expand TSA's awareness and understanding of the current security posture in the passenger rail and mass transit mode, enable more effective targeting of security programs and technical assistance to elevate security, and facilitate sharing of best security practices. TSA TSIs complete these comprehensive assessments by thoroughly reviewing and rating mass transit and passenger rail agencies in 17 Security and Emergency Management Action Items. Updated in 2006, in a collaborative effort by TSA and FTA in coordination with representatives of the mass transit and passenger rail community, the Action Items encompass security and emergency management plans, security program accountability, terrorism prevention and response training and exercises, public awareness campaigns, physical security, personnel security, information security, procedures to elevate security measures as the threat level increases, internal security audits, and operational security measures. As of April 4, 2008, TSA has completed 63 BASE assessments.

The detailed reports TSIs produce of results of BASE assessments provide the data for analysis of areas and trends requiring improvement, both in individual mass transit and passenger rail agencies and nationally based on a consolidation of results. The insight gained from this material informs development of security programs and allocation of resources to address security challenges. The points that follow illustrate this effort. Additionally, TSIs identify and summarize the most effective security practices developed and implemented by mass transit and passenger rail agencies. This information has enabled TSA to produce a compilation of Smart Security Practices derived from the 63 BASE assessments completed to date. The compilation presents 55 smart practices in total, grouped among six strategic priorities: regional partnerships and information sharing; use of random, unpredictable deterrence; advancing the security baseline; technology applications to mitigate high consequence risk; and public awareness and preparedness campaigns. Most significantly, for each smart practice the compilation identifies the agency and one or more officials of the agency that security professionals in the mass transit and passenger rail community may consult for more details and assistance on development and implementation of the practice. Following coordination with the Transit Policing and Security Peer Advisory Group, TSA is distributing the Smart Security Practices throughout the mass transit and passenger rail community by multiple means.

*BASE Assessment Results Drive Program Goals*

Well-trained employees are a force multiplier for security efforts implemented by mass transit and passenger rail agencies. When the BASE results demonstrated the need for significant improvement in continuing security training of employees, TSA developed and published the Mass Transit Security Training Program in February 2007. Produced in coordination with DHS Federal Emergency Management Agency (FEMA), FTA, the Mass Transit Sector Coordinating

Council (SCC), and the Peer Advisory Group, this program provides detailed guidelines on implementing an effective security training program citing the subject areas in which particular categories of employees should receive training. Identified course options include programs funded by FTA/TSA (transit specific terrorism prevention and response) and FEMA (general terrorism prevention and response). Supported by the Transit Security Grant Program, this initiative expanded significantly the volume and quality of training for transit employees. As an example, the proportion of grant awards for security training among eligible mass transit and passenger rail agencies in Tier 2 under the Transit Security Grant Program rose from 3 percent of the total funding allocation in fiscal year (FY) 2006 to 68 percent in FY 2007.

As a strategic priority, TSA emphasizes the expansion of random, unpredictable security activities to enhance deterrence. The BASE results indicated the need for greater effort to assist mass transit and passenger rail agencies in higher risk areas to implement these types of measures. Through the operational package under the Transit Security Grant Program, DHS now funds projects to assemble, train, and equip dedicated anti-terrorism teams to operate in mass transit and passenger rail systems. The specialized expertise these teams develop enhances security through their operational activities, by providing training, and through sharing their experience with other law enforcement officers and employees in their organizations.

Building on the BASE assessment results, which show mass transit and passenger rail agencies conduct and participate regularly in drills and exercises, TSA enhances the focus of these activities on terrorism prevention and immediate response for threats and incidents within the systems. In partnership with agencies in the National Capital Region, TSA is developing a multi-phased, multi-jurisdictional, and cross-functional anti-terrorism exercise program. TSIs in the region are directly involved in this effort. The objective is to produce a package to facilitate planning, preparation, and execution of terrorism prevention and immediate response exercises that can be adapted and implemented by mass transit and passenger rail agencies nationally. This effort will produce the national exercise program required under the 9/11 Commission Act. Drills and exercises are among the priorities for funding in the Transit Security Grant Program.

In addition to conducting the comprehensive security assessments discussed immediately below, the surface inspection force has completed nearly 1,350 profiles of mass transit and passenger rail stations and terminals; secured train-the-trainer certification in terrorist behavior awareness for numerous Transportation Security Inspectors (TSIs); provided training in rail operations awareness to Federal Security Directors and Federal Air Marshals; and conducted more than 13,000 hours of liaison and outreach activities to enhance security in individual agencies and expand regional security collaboration.

TSIs participate actively in regional security forums in their areas, including the classified threat and analysis briefings with mass transit and passenger rail security officials and their Federal partners. These sessions, held on a quarterly basis or as threat developments warrant, take place simultaneously in 15 metropolitan areas through the Federal Bureau of Investigation's (FBI) secure video teleconference system in the Joint Terrorism Task Force (JTTF) network. Intelligence officers from the FBI, DHS, and TSA present information up to the Secret level on threats, incidents, and developments relevant to mass transit and passenger rail. Bringing together the systems' law enforcement chiefs, security directors, and other officials with their

Federal counterparts in DHS, TSA, and the FBI, advances the TSA strategic priority of expanding regional collaboration.

Collectively, these activities reflect a well-defined program geared to strategic security priorities, notably expanding partnerships for security enhancement, elevating the security baseline, building security force multipliers, and ensuring information leadership. Follow-on assessments and smart security practices drawn from the BASE results demonstrate that security posture has improved significantly in mass transit and passenger rail since the TSIs commenced this comprehensive effort. All of these actions, and the results they have achieved, have occurred without "comprehensive security regulations."

The report states most transit stakeholders "had participated in many different TSA assessment and system reviews, but unless such assessments were tied to grant funds to address the vulnerabilities that TSIs had identified …were not certain how TSA was using the information the TSIs were gathering." TSA does not contest that the OIG received feedback to this effect, but the report again fails to present the full context of TSA's efforts in this area.

The BASE program is TSA's primary security assessment tool. As demonstrated by the discussion of specific application of the information gained through the BASE assessments, the results have been applied to advance security program development and resource allocations, including the setting of priorities and their implementation under the Transit Security Grant Program, and to produce a compilation of smart security practices for distribution to the mass transit and passenger rail security partners nationally. Notably, TSNM Mass Transit and the STSIP have made a concerted effort to ensure our security partners are aware of how information collected in the BASE reviews is utilized. STSIP'S Branch Chief briefed the consolidated national BASE results at the Transit Safety and Security Roundtable (attended by law enforcement chiefs and security directors of the largest 50 mass transit and passenger rail agencies) in Chicago in July 2007, and at the National State Safety Oversight Agency conference in Minneapolis in September 2007. In presentations at the July and December 2007 Transit Safety and Security Roundtables and in consultations with the Transit Policing and Security Peer Advisory Group and the Mass Transit SCC, TSNM Mass Transit specifically cited the BASE assessment results as the driving force behind multiple programs, including development of the Mass Transit Security Training Program, the security training initiative and anti-terrorism operational packages funded under the Transit Security Grant Program, and transit system-focused terrorism prevention and response exercises-- notably the ongoing effort to develop a national exercise program with mass transit and passenger rail systems in the National Capital Region. Many of the agencies that have undergone BASE assessments have assisted TSA in producing a compilation of smart security practices derived from the results by consulting on, supplementing, and approving descriptions of security measures identified by TSIs as among the most effective in the Nation.

*Effective Communication*

The report is critical of communication between TSA headquarters and TSIs, concluding that failures in this regard have undermined the credibility of TSIs with security partners in mass transit and passenger rail. In doing so, however, the report once again fails to present the

necessary context, specifically the multi-faceted means by which policymakers inform TSIs of strategies, plans, and programs.

- Mass Transit division representatives, including the Deputy General Manager, participate in the weekly or biweekly conference calls the STSIP holds with the Assistant Federal Security Directors (AFSD)-Surface around the country. During these calls, mass transit and passenger rail security programs and initiatives are discussed, including most notably the BASE program and use of its results in the development of security programs and allocation of resources, such as grant funding.

- Through this forum, Transportation Sector Network Integration (TSNI) officials brief the annual grant program guidance. To ensure they remain aware of developments throughout the grant cycle, TSIs are welcome participants in the regular grant program teleconferences held for stakeholders. Inspectors serve as panelists for grant review activities. In a number of regions, TSIs are key participants in Regional Transit Security Working Group sessions. The groups convene regularly in higher risk areas around the country in a collaborative process with TSA to identify security priorities and reach agreement on funding of the most effective risk mitigation projects.

- TSNM Mass Transit participates in meetings the STSIP holds with AFSDs-Surface and other TSIs at TSA headquarters as well as in the STSIP annual national conferences attended by all surface inspectors. In each of these forums, detailed discussions of security policies, programs, and developments occur.

- The Chief of the STSIP and his designees participate in the Mass Transit Security Information Network, an interagency group consisting of representatives from DHS, TSA, and FTA that analyzes developing situations and produces timely, accurate information products for Federal decision-makers and security officials in mass transit and passenger rail agencies during periods of heightened threat or security incidents. The network also ensures awareness and coordination of activities to harness efforts and avoid duplication.

- Daily communication and coordination occurs between TSNM Mass Transit and STSIP leadership to ensure alignment of security policies and programs. Notifications and information exchange occur on an almost daily basis as well as when incidents of potential security concern are reported in mass transit or passenger rail systems nationally.

- Close coordination with TSNM Mass Transit and the Transportation Security Operations Center (TSOC) is evident in deployment and liaison actions that occur during periods of threat, security incidents, or other emergencies.

- TSIs participate with TSNM Mass Transit representatives in the ongoing effort to develop security standards. This process brings together subject matter experts from mass transit and passenger rail agencies, the American Public Transportation Association, and Federal security partners at TSA and FTA in a joint effort. Current working groups focus on producing standards in three areas – infrastructure protection, emergency management, and risk assessment and management. This initiative should produce multiple consensus

standards during 2008. TSA plans to provide the smart practices derived from the BASE assessment results to the appropriate working groups to spur further progress.

- TSIs are key participants in the classified threat and analysis briefings of mass transit and passenger rail security officials and their Federal partners. These sessions, held on a quarterly basis or as threat developments warrant, take place simultaneously in 15 metropolitan areas through the FBI's secure video teleconference system in the Joint Terrorism Task Force (JTTF) network. TSIs are present to receive the presentations, raise questions, and discuss security implications with law enforcement chiefs and security directors of mass transit and passenger rail agencies in their area as well as regional Federal counterparts from DHS, TSA, and the FBI. As such, TSIs are engaged in advancing the TSA strategic priority of expanding regional collaboration.

- Finally, TSNM Mass Transit generally attempts to coordinate engagement with stakeholders through the TSIs. Notable examples include the collaborative efforts to produce a compilation of smart security practices derived from the BASE assessment results and to develop the national exercise program for mass transit and passenger rail.

- In summary, coordinating through the Office of Security Operations Compliance Division, TSNM Mass Transit and the TSIs have forged an effective partnership for security enhancement. TSIs play integral roles in advancement of multiple strategic security priorities. Without this collaboration, the achievements detailed thoroughly in this response and the technical comments previously provided could not have been achieved.

**The Report Fails to Address the Significant Progress Made by the VIPR Program**

TSA does not believe the report adequately conveys the effectiveness of the VIPR program. As indicated in the report, TSA officials did conduct a productive dialogue with the OIG concerning the program. However, problems remain in the report's treatment of the program. In multiple places, the report reaches conclusions about the VIPR program which appear to be based on singular occurrences, opinion and anecdote, and do not accurately reflect the program as a whole. Additionally, the language employed by the OIG misconstrues some events that occurred during an emergency deployment in the infancy of the VIPR program.

The report conveys the impression that TSA began the VIPR program in July 2007. In fact, TSA formally introduced the program in December 2005. Since that time, hundreds of successful deployments in mass transit and passenger rail systems have taken place, augmenting security with varying force packages of Federal Air Marshals (FAMs), TSIs, Transportation Security Officers (TSOs), Behavior Detection Officers (BDOs), Explosives Security Specialists (ESSs), and explosives detection canine teams, each with supporting equipment.

In describing VIPR program interaction with transit partners, the report states, "[T]he level of assistance transit systems request depends on a transit system's local political and security environment." Decisions to deploy VIPR assets are premised upon a number of factors, including active deterrent value, unpredictability, force composition, and intelligence, taking into account available TSA assets. These factors are tailored to each local transit system's unique security concerns. Political calculations are not, and cannot be, a part of TSA's decision to

deploy VIPR teams. To suggest otherwise indicates a fundamental misunderstanding of the VIPR concept and the value of TSA's deployments.

Notably, the OIG reports cites a July 11, 2007, letter from an external advocacy group, the Federal Law Enforcement Officer's Association, as authoritative proof that VIPR deployments are "*clearly a waste of scarce Federal Air Marshal resources.*" (Report p. 23) The OIG chose to include this opinion despite the fact that since the July 2007 VIPR deployments, Congress has explicitly endorsed and approved the use of FAMs in VIPR operations.

Finally, the OIG report focuses the majority of its assessment regarding the VIPR program on a single series of emergency deployments which occurred 10 months ago. As the report indicates, the July 2007 deployments did occur with very limited notice and advance coordination.

The July 2007 deployments were an immediate response to the terrorist activity in London and Glasgow. On 30 June 2007, two men drove a dark green Jeep Cherokee loaded with propane canisters and fuel through the doors of the passenger terminal of the Glasgow International Airport in an attempted car bombing. This event, along with other intelligence information, raised significant concerns for the safety of the traveling public during the busy July 4 holiday week, both by air and those congregating in mass transit systems for holiday events. As a result, TSA elected to move quickly to surge resources to provide additional security resources to airport and mass transit operators through the VIPR program. Over 100 VIPR exercises were run in the course of a two week period.

The important lesson that TSA and mass transit drew from the July VIPRs was that these kinds of operations needed to occur on a frequent basis so that TSA and local agencies would be ready to respond to these types of threats. Moreover, the Report scrutinizes isolated incidents from the July deployment to support the proposition that the program has elemental flaws, when in fact, approximately 200 transit and aviation VIPR deployments had occurred previously. Indeed, the OIG recognizes that since the July deployments, substantial improvements have been made, which indicates that TSA has addressed significant issues concerning the July deployments. The report creates confusion regarding the true state of the VIPR program, because much of this section of the Report emphasizes the already resolved issues of the July deployments.

TSA absorbed numerous "lessons learned" from the July 2007 deployments. VIPR deployments have improved considerably since these emergency deployments occurred. Achievements include: the establishment of the Joint Coordination Center (JCC), revision of its concept of operations, and improvements in collaborating and communicating with the manifold mass transit and passenger rail security partners, including the Transit Policing and Security Peer Advisory Group.

Two key products have resulted from this collaborative effort. First, TSA – with representatives from OLE/FAMS, TSNM Mass Transit, and the Office of Security Operations, including the Chief of the STSIP and two senior TSIs – and the Peer Advisory Group produced operating guidelines for coordination, planning, preparation, execution, and after action review of VIPR deployments in mass transit and passenger rail systems. These guidelines, finalized in October 2007, have been distributed to Federal Security Directors (FSDs), Federal Air Marshal Special Agents in Charge (FAMSACs), and law enforcement chiefs and security directors in mass transit

and passenger rail agencies. Second, following a thorough presentation on the VIPR program at the December 2007 Transit Safety and Security Roundtable, TSA produced an informational product for mass transit and passenger rail security partners that summarizes the roles and capabilities of each of the available VIPR team elements and provides recommendations on effective deployment. These recommendations aim to facilitate the most effective application of the flexible deterrent resource VIPR teams provide. TSA distributed this product to FSDs, FAMSACs, and law enforcement chiefs and security directors in mass transit and passenger rail agencies in March 2008. Efforts to develop additional informational products are ongoing.

**The Report Ignores Other Significant Mass Transit Security Improvements**

Finally, the report's broad conclusions based on perceived failings in particular aspects of distinct programs convey the impression that the overall mass transit and passenger rail security program suffers from significant shortcomings Again, discussion of the broader context is essential to ensure TSA's program is judged on its full merits. Beyond the programs and initiatives discussed thus far in this response, TSA acted in numerous additional ways to execute its responsibility for mass transit and passenger rail security.

- Within weeks of the March 2004 bombings of commuter trains in Madrid, TSA issued security directives to enhance security in passenger rail systems. The May 2004 directives represented TSA's first such action outside the aviation mode. TSA has reviewed passenger rail agencies' compliance with the multiple measures specified in the directives in both focused Security Directive Reviews and broader security assessments conducted by surface transportation security inspectors. Promulgation of the regulation on security plans mandated by the 9/11 Commission Act will supersede the directives.

- Since 2004, TSA has partnered with FTA to hold twice yearly Transit Safety and Security Roundtables. These sessions bring together the law enforcement chiefs and security directors of the 50 largest mass transit and passenger rail agencies with their Federal security partners from TSA, FTA, and DHS' FEMA in a working group format to discuss security challenges and effective solutions. The 3-day forums engage the collective expertise and experience of the responsible Federal officials and the professionals responsible for security in agencies that transport more than 75 percent of the Nation's users of mass transit and passenger rail.

- To enhance coordination with stakeholders and within government, TSA established the Transit, Commuter and Long Distance Rail Government Coordinating Council (GCC) and recognized the SCC. Additionally, TSA engaged the expertise of security professionals in the mass transit and passenger rail community by forming the Transit Policing and Security Peer Advisory Group. The GCC, created pursuant to the National Infrastructure Protection Plan (NIPP) and consisting of representatives of TSA, DHS, FTA, and the FBI, ensures timely and effective coordination of Federal security enhancement programs and initiatives. The SCC, also formed pursuant to the NIPP, provides security partners in the mass transit and passenger rail community with a forum to consult on security matters and coordinate with the Federal government. Membership includes general managers and chief executive officers of multiple mass transit and passenger rail agencies and representatives of the American Public Transportation Association (APTA), the Community Transport

Association of America (CTAA), and the Amalgamated Transit Union (ATU). The Peer Advisory Group, consisting of 15 law enforcement and security chiefs from mass transit and passenger rail agencies around the country, serves as a consultative body to facilitate TSA's identification of security priorities and development and implementation of effective security enhancement programs and initiatives.

- TSA and FTA collaborated, in coordination with the mass transit and passenger rail community through the SCC and the Peer Advisory Group to update and publish the Recommended Protective Measures for Homeland Security Advisory System (HSAS) Threat Levels in November 2006. This product details the types of measures mass transit and passenger rail agencies should integrate into their security plans to ensure an effective level of security at the various threat levels in HSAS. Numerous agencies have relied on this product in contingency planning and in implementation of enhanced security measures in response to threats and attacks, attempts, or disrupted plots overseas.

- TSA convened and led an interagency initiative to assess risk and prioritize mitigation efforts for all underwater tunnels used by passenger rail systems in the United States. The National Tunnel Security Initiative brings together subject matter experts from DHS and DOT agencies to identify, assess, and prioritize the risk to the nation's 29 underwater passenger rail tunnels. It assists the transit and rail agencies in planning and implementing protective measures to deter and prevent attacks as well as blast mitigation and emergency response strategies in the event of a terrorist attack and/or all hazards incident or event. The interagency group has developed mitigation strategies, engaged stakeholders, analyzed and applied the results of risk assessments, prepared statements of work for testing and modeling programs, and integrated the overall risk mitigation effort for a cohesive, coordinated, and effective approach. The initiative has identified and assessed risk to underwater tunnels, prioritized tunnel risk mitigation based on risk to drive grant funding to the most pressing areas, developed strategies for funding future technology research and development aimed at producing novel approaches to this challenging problem, and recommended protective measures transit agencies may implement with available resources or through targeted grant funding. To advance this concerted effort, the Transit Security Grant Program makes projects to protect high risk underwater and underground assets and systems a top funding priority.

- In collaborative efforts with TSA's Office of Security Technology and the Department's Directorate for Science and Technology, TSA pursues research and development of technological solutions to security challenges in mass transit and passenger rail. This multi-faceted effort advances risk mitigation projects in several key areas, including protection of underwater transit tunnels, anomaly and explosives detection, chemical and biological hazard detection and response, visual surveillance and monitoring capabilities, transit vehicle control, and protection of supervisory control and data acquisition (SCADA) systems.

- Lastly, the NEDCTP, deservedly recognized for its effectiveness in the report, has deployed more than 50 canine teams among 14 mass transit and passenger rail agencies throughout the country on a risk-informed basis. Though accurately describing the program in most respects, the report does erroneously state TSA provides "secure

containers for storing explosive training materials." Rather, the NEDCTP has always supplied and delivered two full-size explosives magazines for the storage of explosive training aids at no cost to the participating mass transit or passenger rail agency. TSA also supplies and delivers fresh explosive training aids annually at no cost to each participating agency. Overall, the NEDCTP provides an exceptional resource whose mobility and random, unpredictable employment advances deterrence.

Collectively, the activities discussed in this response demonstrate well TSA's execution of its security oversight and operational security enhancement responsibilities.

Conclusion

TSA believes that progress has been and continues to be made in security for mass transit and passenger rail systems. The detailed programs listed in this memorandum provide a more accurate picture of these programs than the portrayal provided by the OIG review. TSA looks forward to working with OIG to advance the continuing improvement that best serves the public interest. TSA generally concurs with and has already taken steps to address several of the recommendations set forth in the OIG report. TSA's specific responses to the recommendations contained in the draft report accompany this memorandum.

**Transportation Security Administration (TSA) Draft Report**
**Office of the Inspector General (OIG) Draft Report OIG-07-XX, "TSA's Administration and Coordination of Mass Transit Security Programs," February 2008**

**Recommendation 1:** Place the Surface Transportation Security Inspection program under the direct authority of a TSA headquarters official who is responsible for surface transportation, such as the Office of Security Operations' Assistant General Manager for Compliance.

**TSA Does Not Concur:** Since its inception in 2005, the Surface Transportation Security Inspection Program (STSIP) has been under the direct authority of the Office of Security Operations (OSO), Office of Compliance. While the Office of Compliance oversees the Surface Transportation Security Inspection Program and directs the work plan, training, and other aspects of field inspector activity, the reporting line of all TSIs in field deployment is to designated Federal Security Directors (FSDs) who report to the General Manager for Field Operations, OSO. The FSDs are the operational field component of the Office of Security Operations and are charged with the implementation of all field operational activities.

The STSIP office informs FSDs of TSI priorities and programs through dissemination of an annual work plan written by the STSIP in close coordination with TSNM and via written directives and communications distributed through the OSO Net Hub system and other means. The STSIP office has also developed an executive training course for FSDs that is held periodically at Transportation Technology Center, Inc. (TTCI) in Pueblo, CO. Additionally, FSDs are kept informed of key activities and programs of the TSIs nationally by a written summary report issued weekly by the STSIP office. Assistant Federal Security Directors (AFSDs)-Surface participate in weekly or bi-weekly national conference calls hosted by the STSIP office and inform FSDs within their respective regions of new or changing processes in STSIP programs. AFSDs-Surface and local lead TSIs are required to attend FSD meetings and routinely report STSIP activities to FSDs.

In December 2007, OSO reviewed the reporting structure of TSIs. As a result of this review, TSA has taken steps in recent weeks to strengthen and clarify TSI reporting lines, to include revising existing work rules to allow for clearer definitions of roles and oversight responsibilities of the STSIP program office and the FSDs and plans to issue a revised organization chart that clarifies reporting lines of all TSIs and AFSDs-Surface to designated FSDs.

**Recommendation 2:** Direct TSNM to provide TSIs information and updates on the rail-related programs. Invite TSIs to local meetings with stakeholders. Instruct the Office of Security Operations' Compliance Program to make all TSI assessments and profiles available to employees of TSNM.

**TSA Concurs in Part:** First, the OIG recommendation to direct OSO's Compliance Program to make all TSI assessments and profiles available to employees of TSNM infers that such access has been denied to TSNM. All TSI assessments are readily available to TSNM, both through pre-arranged direct access and upon request, the results of which are being used by TSNM to set the priorities, benchmarks, and goals for security programs. Since 2006, the STSI Program

Office has provided TSNM with full and unfettered access to the BASE assessments and station profiles. No request for access to TSI assessments from TSNM has ever been denied by the Office of Compliance. This assessment information is critical as grant priorities are established and smart security practices are reviewed and updated. The results of the BASE assessments for particular systems are not routinely shared with other agencies or departments unless they are given permission by the assessed mass transit or passenger rail system.

Within TSNM, access to assessment results by TSNM employees is determined on a "need to know" basis in connection with their official duties. The policy reflects the approach developed and agreed between TSNM Mass Transit and the STSIP to ensure protection of critical security information. An overriding concern is avoiding loss of control of BASE results reports and station profiles that could well result from saving of files on hard drives, CD-ROMs, or other removable devices and from production of numerous hard copies stored in multiple offices and other locations. This policy specifically aims to prevent the negligent disclosure of this sensitive security information. TSNM Mass Transit provides access to hard copies of BASE results reports and station profiles to those whose duties, such as grants personnel in TSNI, warrant review of a mass transit or passenger rail agency's security status. These personnel can also receive copies of the national compilation of BASE results produced by the STSIP. A briefing on those results, with slides depicting overall status nationally in each Security and Emergency Management Action Item, was presented at the Transit Safety and Security Roundtable in July 2007, which was attended by TSNM Mass Transit and TSNI personnel.

Second, TSNM Mass Transit coordinates and communicates thoroughly with TSIs.

- Mass Transit division representatives, including the Deputy General Manager, participate in the weekly or biweekly conference calls the Branch Chief of the Surface Transportation Security Inspection Program (STSIP) holds with the AFSDs-Surface around the country. During these calls, mass transit and passenger rail security programs and initiatives are discussed, including most notably the BASE program and use of its results in the development of security programs and allocation of resources, such as grant funding.

- Through this forum, Transportation Sector Network Integration (TSNI) officials brief the annual grant program guidance. To ensure they remain aware of developments throughout the grant cycle, TSIs are welcome participants in the regular grant program teleconferences held for stakeholders. Inspectors serve as panelists for grant review activities. In a number of regions, TSIs are key participants in Regional Transit Security Working Group sessions. The Groups convene regularly in higher risk areas around the country in a collaborative process with TSA to identify security priorities and reach agreement on funding of the most effective risk mitigation projects.

- TSNM Mass Transit participates in meetings the STSIP holds with AFSDs-Surface and other TSIs at TSA HQs as well as in the STSIP annual national conferences attended by all surface inspectors. In each of these forums, detailed discussions of security policies, programs, and developments occur.

- The Chief of the STSIP and his designees participate in the Mass Transit Security Information Network, an interagency group consisting of representatives from DHS, TSA,

and FTA that analyzes developing situations and produces timely, accurate information products for Federal decision-makers and security officials in mass transit and passenger rail agencies during periods of heightened threat or security incidents. The network also ensures awareness and coordination of activities to harness efforts and avoid duplication.

- Daily communication and coordination occurs between TSNM Mass Transit and STSIP leadership to ensure alignment of security policies and programs. Notifications and information exchange occur on an almost daily basis as well as when incidents of potential security concern are reported in mass transit or passenger rail systems nationally.

- Close coordination with TSNM Mass Transit and the TSOC is evident in deployment and liaison actions that occur during periods of threat, security incidents, or other emergencies.

- TSIs participate with TSNM Mass Transit representatives in the ongoing effort to develop security standards. This process brings together subject matter experts from mass transit and passenger rail agencies, the American Public Transportation Association, and Federal security partners at TSA and FTA in a joint effort. Current working groups focus on producing standards in three areas – infrastructure protection, emergency management, and risk assessment and management. This initiative should produce multiple consensus standards during 2008. TSA plans to provide the smart practices derived from the BASE assessment results to the appropriate working groups to spur further progress.

- TSIs are key participants in the classified threat and analysis briefings of mass transit and passenger rail security officials and their Federal partners. These sessions, held on a quarterly basis or as threat developments warrant, take place simultaneously in 15 metropolitan areas through the FBI's secure video teleconference system in the Joint Terrorism Task Force (JTTF) network. TSIs are present to receive the presentations, raise questions, and discuss security implications with law enforcement chiefs and security directors of mass transit and passenger rail agencies in their area as well as regional Federal counterparts from DHS, TSA, and the FBI. As such, TSIs are engaged in advancing the TSA strategic priority of expanding regional collaboration.

- Finally, TSNM Mass Transit generally attempts to coordinate engagement with stakeholders through the TSIs. Notable examples include the collaborative efforts to produce a compilation of smart security practices derived from the BASE assessment results and to develop the national exercise program for mass transit and passenger rail.

- In summary, coordinating through the Office of Security Operations Compliance Division, TSNM Mass Transit and the TSIs have forged an effective partnership for security enhancement. TSIs play integral roles in advancement of multiple strategic security priorities. Without this collaboration, the achievements detailed thoroughly in this response and the technical comments previously provided could not have been achieved.

**Recommendation 3:** Develop specific, feasible security standards for mass transit systems. Incorporate applicable TSI assessments, and consult with DOT and relevant transit associations, such as the American Public Transportation Association (APTA), when developing these standards.

**TSA Does Not Concur:** The recommendations to consult with DOT and APTA are clearly already in practice, but the recommendations leave out the two most important consultations, intelligence and law enforcement entities. TSA and the Federal Transit Administration (FTA) have participated with APTA in a security standards development process that began in January 2006. FTA has funded this effort extensively, in excess of $1 million. TSNM Mass Transit and TSIs have provided subject matter expertise to the joint working groups, which cover three areas: infrastructure protection, emergency management, and risk management. TSA plans to provide the smart practices derived from the BASE assessment results to the appropriate working groups to spur progress and expedite completion of this lengthy collaborative effort. This initiative, coupled with separate working group efforts, should produce multiple consensus standards in 2008.

Additionally, TSA has worked cooperatively with Federal security partners and the mass transit and passenger rail community to develop and disseminate products to guide and facilitate security enhancement activities. These include the Security and Emergency Management Action Items (implementation of which are assessed through the BASE program), the Recommended Protective Measures for HSAS Threat Level, and Security Measures for Transit Tunnels. TSA has compiled the smart practices derived from the BASE assessment results to produce a compilation for national dissemination to inspire communications among professional colleagues to produce adaptation and widespread implementation. As these products reflect some of the most effective practices in the mass transit and passenger rail community, this effort is akin to standards development.

**Recommendation 4:** Develop procedures for incorporating asset-specific risk and vulnerability assessments, including information provided by TSIs, into the grant decision making process and grant guidance. Designate a TSI from each major field office to provide updates to Transportation Sector Network Management on the status of grant projects.

**TSA Concurs:** TSA is already incorporating system-specific security assessments and other information secured by TSIs into the processes of defining grant program priorities, developing security programs, and allocating resources. Utilization of TSIs in oversight of grant project status is seen by TSA as a key component of the overall strategic approach to security enhancement in mass transit environments, and as such, OSO will work with TSNM to develop a plan to initiate such activity in the future. TSI staffing is being increased by an additional 75 inspectors in FY 2008, which will reduce the burden of initiating the new field inspection component.

**Recommendation 5:** In TSA's annual report to Congress on how it used grants to implement its transportation security goals, TSA should include each grant recipient's assessment of the grant application and award process.

**TSA Concurs in Part:** Including an assessment from every eligible mass transit and passenger rail agency on grant program administration and the application and award processes would prove unduly time-consuming and burdensome. Feedback from eligible grant applicants should inform program improvements. The annual report should summarize this feedback – pro and

con – as part of the presentation to Congress on the grant program's effectiveness and needed improvements.

**Recommendation 6:** Seek Memorandums of Agreement with all relevant transit authorities regarding VIPR deployments. These Memorandums of Agreements should: describe a Concept of Operations or Standard Operating Procedure for both planned and unforeseen events; explain how TSA personnel will communicate with transit authorities and other local law enforcement; and identify the legal authorities that VIPR team members will have in the event of an emergency. The Memorandums of Agreement should specify that participation in VIPR exercises is voluntary and at the request of the local transit authority.

**TSA Concurs in Part:** TSA agrees that much of the requested information set forth in this recommendation is beneficial to the VIPR deployment process. This process already contains the information described, in concept of operations plans, in specific operations plans, and in targeted informational materials. Additionally, specific concerns between TSA and its transit partners are routinely addressed by local points of contact and with FAMSACs and FSDs. We note that TSA does discuss the concept of operations with the local authorities and operators, who have the opportunity to offer changes. No VIPR deployment is executed without a written concept of operations. The concept of operations reflects the agreed upon plan. Further, a requirement for a formal Memorandum of Agreement (MOA) for each individual VIPR deployment would likely mean serious delays in operational deployments, hindering VIPR performance and perhaps adversely impacting the program's overall effectiveness.

TSA respectfully non-concurs with the suggestion that MOAs "specify that participation in VIPR exercises is at the request of the local transit authority." There is no requirement in the 9/11 Commission Act or elsewhere that VIPR operations be conducted "at the request of the local transit authority." VIPR operations are conducted on a cooperative basis with local transit and law enforcement stakeholders, and the process has greatly improved since the emergency deployments of July 2007. The language suggested by the report would unduly limit TSA's options in a manner seemingly inconsistent with the Congressional mandates and authorities established by the Aviation and Transportation Security Act, the 9/11 Commission Act, and recent Appropriations enactments.

The other steps proposed by the OIG have already taken place through the collaborative effort within TSA and between TSA and the mass transit and passenger rail community to improve coordination, preparation, planning, execution, and after action review of VIPR deployments. The operating guidelines set in the "Effective Deployment of Visible Intermodal Prevention and Response Teams in Mass Transit and Passenger Rail" reflect the collaborative efforts of TSA and the mass transit and passenger rail community represented through the Transit Policing and Security Peer Advisory Group. Approved on October 30, 2007, these guidelines encompass 10 functional areas essential to effective security augmentation deployments under the VIPR program in mass transit and passenger rail systems. The functional areas are Coordination, Mission Focus, Active Deterrence, Planning, Force Composition, Consistency, Training, Communication, Authority, and Continuous Improvement.

These functional areas allow flexibility for regional TSA officials and law enforcement chiefs and security directors in mass transit and passenger rail agencies to work collaboratively in light

of local operating circumstances. A one-size-fits-all approach from TSA headquarters is neither advisable nor effective. The guidelines aim to ensure regional TSA officials and law enforcement chiefs and security directors in mass transit and passenger rail agencies have the flexibility to gear coordination, preparation, planning, and execution of VIPR operations to the unique conditions that apply in their operating areas.

Addressing specific components of Recommendation 6:

- Among the activities to advance "Coordination," the operating guidelines state that "Mass transit and passenger rail agencies and regional TSA officials may enter into memoranda of agreement or understanding to set guiding principles for the operational engagement of TSA VIPR capabilities with system law enforcement and security capabilities." This should provide a broad framework sufficient for local stakeholders.
- The section in the operating guidelines on "Communications" addresses the subject on multiple levels: regular engagement between regional TSA officials and the security leads in a mass transit or passenger rail system; interoperable tactical communications to ensure effective execution of VIPR deployments; and public communications – the media components – with the importance of ensuring focus is on the mass transit or passenger rail system as lead to depict its security program broadly.
- In the "Authority" section, the operating guidelines address TSA's authority to implement the VIPR program, the legal authorities of FAMs in mass transit and passenger rail, the lead role the law enforcement agency for the system maintains, and the availability of the TSA Office of Chief Counsel to assist operating, security, and legal officials in mass transit and passenger rail agencies on issues and questions pertaining to Federal authorities underlying the VIPR program and its activities.

To improve communications and enhance the effectiveness of VIPR deployment, the operating guidelines for VIPR deployments in mass transit and passenger rail systems have been distributed to FSDs, AFSDs-Surface, and FAMS SACs around the country by the JCC. At the Transit Safety and Security Roundtable held in Los Angeles in December 2007, the guidelines provided the foundation for a detailed presentation on and discussion of VIPR program capabilities and their effective use in mass transit and passenger rail systems. The guidelines have been disseminated to the law enforcement chiefs and security directors of the largest 50 mass transit and passenger rail agencies and other stakeholders in attendance.

To build on the progress made at the Roundtable, TSA produced a white paper on the roles and capabilities of the various VIPR team elements with guidance on their effective deployment for deterrent effect in mass transit and passenger rail systems. This paper has been disseminated to FSDs and FAMSACs and law enforcement chiefs and security directors in mass transit and passenger rail agencies to facilitate their engagement to expand the scope and effectiveness of VIPR deployments in this mode. It has also been provided to each of the AFSDs-Surface (Senior TSIs) for use in their regular liaison with security officials in mass transit and passenger rail agencies. Finally, TSA is providing focused training in anti-terrorism techniques for its VIPR team members that will enhance their effectiveness in detection and deterrence and provide a model for adoption of similar practices by security forces in mass transit and passenger rail systems.

These efforts demonstrate the substantial enhancement in cooperation on and coordination of VIPR deployments between TSA and mass transit and passenger rail agencies.

**Recommendation 7:** Revise the grant program eligibility criteria to allow start-up funds for mass transit systems that do not already have a canine explosive detection unit.

**TSA Concurs:** The Transit Security Grant Program (TSGP) project and funding criteria already allow reasonable and defined start-up costs to mass transit and passenger rail systems for initial deployment of canine explosives detection teams.

Under the TSGP, eligible mass transit and passenger rail agencies may receive $150,000 per team per year through FY 2010. These funds are adequate for start-up and sustainment costs for the covered period. Only agencies that do not train or certify under the TSA National Explosives Detection Canine Team Program (NECDTP) are eligible to receive TSGP funding

Another option available to mass transit and passenger rail agencies is support through the NECDTP. Funding for this program comes through annual appropriations. The NEDCTP covers the costs of the canine and the training of the canine and the assigned handler from the mass transit or passenger rail agency. Additionally, the NEDCTP provides a reimbursement of $40,000 per team, per year to cover sustainment costs. TSA concurs with the OIG's recommendation as it pertains to the NEDCTP and its state/local partners.

## Appendix C
## BASE Assessment Criteria

| | TSA Baseline Assessment for Security Enhancement (BASE) Criteria |
|---|---|
| 1 | Establish written security programs and emergency management plans |
| 2 | Define roles and responsibilities for security and emergency management |
| 3 | Ensure that operations and maintenance supervisors, forepersons, and management are held accountable for security issues under their control |
| 4 | Coordinate Security and Emergency Management Plan(s) with local and regional agencies |
| 5 | Establish and maintain a Security and Emergency Training Program |
| 6 | Establish plans and protocols to respond to the DHS Homeland Security Advisory System threat levels |
| 7 | Implement and reinforce a Public Security and Emergency Awareness Program |
| 8 | Conduct tabletop and functional drills |
| 9 | Establish and use a risk management process to assess and manage threats, vulnerabilities and consequences |
| 10 | Establish and use an information sharing process for threat and intelligence information. |
| 11 | Establish and use a reporting process for suspicious activity (internal and external) |
| 12 | Control access to security critical facilities with ID badges for all visitors, employees, and contractors |
| 13 | Conduct physical security inspections |
| 14 | Conduct background investigations of employees and contractors |
| 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 |
| 17 | Conduct Security Plan Audits |

**Source: TSA BASE Template**

## Transportation Sector-Specific Implementation Plan

**(from the *Transportation Sector-Specific Mass Transit Modal Annex*, May 5, 2007, pg. 32-33)**

**1. Protection of high risk/high consequence underwater and underground rail assets.**

Many of the nation's largest transit systems have significant track miles and large concentrations of riders in rail systems that run underground and underwater. It is the highest priority of the FY07 [Transit Security Grant Program] to support measures that will protect underground rail system assets, and particularly underwater assets, from terrorist attack by improvised explosive devices (IEDs) or other threats that can damage or significantly breach such assets. Active coordination and regular testing of emergency evacuation plans can greatly reduce loss of life in serious incidents.

**2. Protection of other high risk/high consequence assets and systems that have been identified through system-wide risk assessments.**

It is imperative that transit agencies focus countermeasure resources on their highest risk, highest consequence areas or systems. The [Transit Security Grant Program] will particularly support development and enhancement of capabilities to prevent, detect and respond to terrorist attacks employing chemical, biological, radiological, nuclear and explosive (CBRNE) weapons, particularly IEDs. For example, a system-wide assessment may highlight the need to segregate critical security infrastructure from public access. One solution could be an integrated intrusion detection system, controlling access to these critical facilities or equipment. Transit systems should consider security technologies to help reduce the burden on security manpower. Using smart [closed circuit television] systems in remote locations could help free up security patrols to focus on more high-risk areas.

**3. Use of visible, unpredictable deterrence.**

Visible and unpredictable security activities instill confidence and enhanced security awareness in the riding public, and deter attacks by disrupting the ability of terrorists to prepare for and execute attacks. Examples include the acquisition, training, and certification of explosives detection canine teams; training of law enforcement, security officials and frontline employees in behavioral pattern recognition; and procurement of mobile detection or screening equipment to identify the presence of explosives or their residue and other suspicious items on persons or in packages.

**4. Targeted counter-terrorism training for key front-line staff.**
Effective employee training programs address individual employee responsibilities and provide basic security awareness to front line employees, including equipment familiarization, assessing and reporting incident severity, appropriate responses to protect self and passengers, use of protective devices, crew communication and coordination, and incident evacuation procedures. For example, well trained and rehearsed operators can help ensure that if an underground station has suffered a chemical agent attack, trains – and the riding public – are quickly removed from the scene, thus reducing their exposure and risk.

**5. Emergency preparedness drills and exercises.**
In order to assess and enhance a system's capability to respond under the variety of serious incidents, transit agencies are encouraged to maintain an emergency drill and exercise program to test key operational protocols including coordination with first responders. The [Transit Security Grant Program] can support exercises related to terrorist attack scenarios (such as IED or CBRNE attacks), natural disasters and other emergencies. Such programs can take various forms, from tabletop exercises to more comprehensive multi-agency full-scale exercises. [Transit Security Grant Program] funds also support rigorous after action assessments to identify further system improvements.

**6. Public awareness and preparedness campaigns.**
A public awareness and preparedness program can employ announcements, postings in stations and transit vehicles or other media to ensure awareness of heightened alert or threat conditions. Effective awareness programs enlist the public in becoming an informal part of an agency security plan. They should explain specific actions the public can take to contribute to strengthening system security.

**7. Efforts in support of the national preparedness architecture.**
Transit agencies are encouraged to take steps to embrace the national preparedness architecture priorities, several of which have already been highlighted as [Transit Security Grant Program] priorities. The following six national priorities are particularly relevant: expanding regional collaboration; implementing the National Incident Management System, the National Response Plan and the National Infrastructure Protection Plan; strengthening information sharing and collaboration capabilities; enhancing interoperable communications capabilities; strengthening CBRNE detection and response capabilities; and improving citizen preparedness capabilities.

| **My mission and my role as a Surface Transit Security Inspector are clearly defined** | | |
|---|---|---|
| Strongly Agree (3) / Agree (22) | 25 | 30% |
| No Opinion (4) | 4 | 5% |
| **Disagree (34) / Strongly Disagree (19)** | **53** | **64%** |
| Do Not Know / N/A (1) | 1 | 1% |
| All | 83 | 100% |

| **The chain of command to my superiors is clearly defined** | | |
|---|---|---|
| Strongly Agree (12) / Agree (16) | 28 | 34% |
| No Opinion | 3 | 4% |
| **Disagree (24) / Strongly Disagree (28)** | **52** | **63%** |
| Do Not Know / N/A | 0 | 0% |
| All | 83 | 100% |

| **My daily responsibilities/duties as a Surface Transportation Security Inspector closely match what I expected before I accepted this position** | | |
|---|---|---|
| Strongly Agree (2) / Agree (22) | 24 | 29% |
| No Opinion | 8 | 10% |
| **Disagree (29) / Strongly Disagree (22)** | **51** | **61%** |
| Do Not Know / N/A | 0 | 0% |
| All | 83 | 100% |

| **When conducting on-site assessments, security reviews, and station profiles, local transit authorities provide me the access and information that I need.** | | |
|---|---|---|
| **Strongly Agree (22) / Agree (52)** | **74** | **89%** |
| No Opinion | 1 | 1% |
| Disagree (3) / Strongly Disagree (3) | 6 | 7% |
| Do Not Know / N/A | 2 | 2% |
| All | 83 | 100% |

| **In order to do my job effectively, I require the authority to make unannounced inspections of rail yards and transit stations/facilities.** | | |
|---|---|---|
| **Strongly Agree (51) / Agree (21)** | **72** | **87%** |
| No Opinion | 1 | 1% |
| Disagree (6) / Strongly Disagree (3) | 9 | 11% |
| Do Not Know / N/A | 1 | 1% |
| All | 83 | 100% |

| **In order to do my job effectively, I require the authority to issue citations for violations of security regulations.** | | |
|---|---|---|
| **Strongly Agree (36) / Agree (34)** | **70** | **84%** |
| No Opinion | 3 | 4% |
| Disagree (6) / Strongly Disagree (3) | 9 | 11% |
| Do Not Know / N/A | 1 | 1% |
| All | 83 | 100% |

| **Local transit authorities use and value the assessments and evaluations that I have performed.** | | |
|---|---|---|
| **Strongly Agree (19) / Agree (43)** | **62** | **75%** |
| No Opinion | 5 | 6% |
| Disagree (5) / Strongly Disagree (6) | 11 | 13% |
| Do Not Know / N/A | 5 | 6% |
| All | 83 | 100% |

| **I have raised security concerns to local transit authorities, which they have subsequently addressed or attempted to address.** | | |
|---|---|---|
| **Strongly Agree (14) / Agree (42)** | **56** | **67%** |
| No Opinion | 8 | 10% |
| Disagree (10) / Strongly Disagree (1) | 11 | 13% |
| Do Not Know / N/A | 8 | 10% |
| All | 83 | 100% |

| **I have sufficient direction and information from my superiors, including local Federal Security Directors and TSA Headquarters personnel, to do my job effectively** | | |
|---|---|---|
| Strongly Agree (4) / Agree (21) | 25 | 30% |
| No Opinion | 12 | 14% |
| **Disagree (23) / Strongly Disagree (23)** | **46** | **55%** |
| Do Not Know / N/A | 0 | 0% |
| All | 83 | 100% |

| **I feel that TSA headquarters uses the information that I provide to make policy decisions or prioritize grant decisions.** | | |
|---|---|---|
| **Strongly Agree (5) / Agree (29)** | **34** | **41%** |
| No Opinion | 10 | 12% |
| Disagree (14) / Strongly Disagree (15) | 29 | 35% |
| Do Not Know / N/A | 10 | 12% |
| All | 83 | 100% |

| **When TSA headquarters officials conduct meetings with transit security stakeholders in my jurisdiction, Surface Transportation Security Inspectors assist with the preparation and are included in the meetings.** | | |
|---|---|---|
| Strongly Agree (2) / Agree (14) | 16 | 19% |
| No Opinion | 8 | 10% |
| **Disagree (24) / Strongly Disagree (28)** | **52** | **63%** |
| Do Not Know / N/A | 7 | 8% |
| All | 83 | 100% |

| **Stakeholders, including state officials and transit authorities, perceive that there is cooperation and coordination between TSA headquarters and Surface Transportation Security Inspectors in the field.** | | |
|---|---|---|
| Strongly Agree (6) / Agree (18) | 24 | 29% |
| No Opinion | 17 | 20% |
| **Disagree (19) / Strongly Disagree (14)** | **33** | **40%** |
| Do Not Know / N/A | 9 | 11% |
| All | 83 | 100% |

| **My various supervisors (Federal Security Directors in the field and TSA headquarters officials) coordinate well with each other when setting my priorities.** | | |
|---|---|---|
| Strongly Agree (2) / Agree (14) | 16 | 19% |
| No Opinion | 10 | 12% |
| **Disagree (21) / Strongly Disagree (33)** | **54** | **65%** |
| Do Not Know / N/A | 3 | 4% |
| All | 83 | 100% |

William McCarron, Chief Inspector, Department of Homeland Security, Office of Inspections

Lorraine Eide, Senior Inspector, Department of Homeland Security, Office of Inspections

Preston Jacobs, Inspector, Department of Homeland Security, Office of Inspections

Tristan Weir, Inspector, Department of Homeland Security, Office of Inspections

**Department of Homeland Security**

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
DHS Component Liaison
Administrator, Transportation Security Administration
TSA Audit Liaison

**Office of Management and Budget**

Chief, Homeland Security Branch
DHS OIG Budget Examiner

**Congress**

Congressional Oversight and Appropriations Committees, as appropriate

## Additional Information and Copies

**To obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254-4199, fax your request to (202) 254-4305, or visit the OIG web site at www.dhs.gov/oig.**

## OIG Hotline

**To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations:**

- **Call our Hotline at 1-800-323-8603;**
- **Fax the complaint directly to us at (202) 254-4292;**
- **Email us at DHSOIGHOTLINE@dhs.gov; or**
- **Write to us at:**
  **DHS Office of Inspector General/MAIL STOP 2600, Attention: Office of Investigations - Hotline, 245 Murray Drive, SW, Building 410, Washington, DC 20528,**

**The OIG seeks to protect the identity of each writer and caller.**