



Mass Transit Modal Annex

Table of Contents

Mass Transit Modal Annex

1	Executive Summary	1
2	Mass Transit and Passenger Rail	3
2.1	Vision for the Mode	3
2.2	Description of Mode	4
2.2.1	Overview	4
2.2.2	Background	Error! Bookmark not defined.
2.2.3	Responsibilities	5
2.2.4	Consequences, Vulnerabilities, and Threats.....	7
2.3	Transit, Commuter and Long-Distance Rail Government Coordinating Council and Sector Coordinating Council Structure and Process.....	8
3	Implementation Plan	9
3.1	Goals, Objectives, and Programs/Processes.....	9
	Expanding Partnerships for Security Enhancement	9
3.1.2	Continuously Advancing the Security Baseline	10
3.1.3	Building Security Force Multipliers	10
3.1.4	Security Information Leadership.....	11
3.1.5	Deploying Tools to Mitigate High Consequence Risks.....	12
3.2	Security Programs and Processes	13
3.2.1	Surface Transportation Security Inspection Program.....	Error! Bookmark not defined.
3.2.2	National Explosives Detection Canine Teams	17
3.2.3	Visible Intermodal Prevention and Response (VIPR) Teams.....	19
3.2.4	Information-Sharing.....	20
3.2.5	Security Training and Awareness Programs	22
3.2.6	National Tunnel Security Initiative	25
3.2.7	Security Technology Deployment.....	25
3.2.8	Technology Research and Development	25
3.2.9	International Initiatives.....	27
3.3	Advancing Security Goals and Objectives	Error! Bookmark not defined.
3.4	Effective Practices, Security Guidelines, Security Standards, and Compliance and Assessments Processes	29
3.4.1	Security Guidelines	29
3.4.2	Security Standards Development.....	30
3.4.3	Security Directives.....	30
3.4.4	Notice of Proposed Rulemaking.....	31
3.5	Grant Programs.....	31
3.6	Way Forward.....	34
3.7	Metrics.....	35
4	Program Management	37
5	Mass Transit and Passenger Rail Security Gaps	39

1 Executive Summary

The mass transit and passenger rail industry and their Federal, State and local partners face many challenges in their efforts to provide a secure and protected public transportation environment. The systems are open, serving millions of passengers every day. The networks cover wide geographical areas providing numerous points of access, transfer, connection to other means of transportation, and egress, leading to high passenger turnover difficult to monitor effectively. As the public and private partners move forward with implementing the plan to secure the mass transit and passenger rail systems, new challenges arise. In this context, public and industry partners seek to provide a secure environment for passengers and employees through training, public outreach, procedures and hardening of physical assets and expanding visible/covert, random, and unpredictable security measures. This plan for mass transit and passenger rail security sets out to achieve the objectives and priorities enumerated in the Transportation Systems Sector Security Plan (TSSP), the Presidential Executive Order 13416, "Strengthening Surface Transportation Security," as well as other national and regional strategies to mitigate transportation risk.

These objectives are achieved by applying risk management principles set forth in the TSSP. This risk management framework ensures that risk-reduction and protection measures are implemented in mass transit and passenger rail systems and assets where they offer the most benefit both in response to specific threats and in the general threat environment. This joint effort takes place through the Transit, Commuter, and Long-Distance Rail Government Coordinating Council (TCLDR-GCC) and the Mass Transit Sector Coordinating Council (SCC). These forums foster effective communications and coordination for the governmental entities and the members of the transit community. The TCLDR-GCC and SCC serve as coordinating bodies to discuss, develop, and refine positions on all matters in transit security. Further, they streamline the coordination process between government and the transit industry, helping to advance a partnership in developing and implementing security programs. Working through the Critical Infrastructure Partnership Advisory Council (CIPAC), government and industry come together in efforts to reach consensus on transit security initiatives.

Within the GCC/SCC framework, mass transit and passenger rail governmental and industry partners have devised, and are implementing, a plan consistent with the approach set out in the NIPP. This plan aims to enhance security through collaborative efforts nation-wide and in regional areas throughout the Nation to employ the full spectrum of security resources in the most effective manner possible. Essential components of the plan include maximizing the power of information, using risk-based principles in conducting assessments of assets and systems, and applying the results to ensure domain awareness and to identify and implement security programs and concrete and specific criteria to measure the effectiveness of these programs. These efforts are advanced in the context of an ever-changing threat environment and encompass proactive measures to reduce vulnerabilities in general and improve overall preparedness to meet a range of contingencies, including response to specific threat intelligence and security incidents.

Critical systems and assets have been identified via a collaborative effort involving the Transportation Security Administration (TSA) and other components within the Department of Homeland Security (DHS), the Federal Transit Administration (FTA), the Federal Railroad Administration (FRA), the Federal Bureau of Investigation (FBI), mass transit and passenger rail agencies, and State and local governments. FTA, TSA, and other DHS components, in cooperation with State, local, and industry security partners have conducted a number of vulnerability assessments of the systems and assets. Rail transit, commuter rail and major transit systems have developed security plans and emergency preparedness plans in a format

that is consistent with the FTA's Public Transportation System Security and Emergency Preparedness Planning Guide (2003). TSA's Surface Transportation Security Inspection (STSI) Program continues these efforts with the Baseline Assessment and Security Enhancement (BASE) program. The BASE Program reviews transit systems implementation of 17 Security and Emergency Preparedness Action Items (security action items), jointly developed by TSA and FTA in coordination with the Mass Transit Sector Coordinating Council. Additionally, the STSI Program offers the Security Analysis and Action Program (SAAP), which constitutes a systematic vulnerability assessment of mass transit or passenger rail systems. The program utilizes several different tools to identify vulnerabilities based on specific scenarios, such as an improvised explosive device (IED) on a passenger train. SAAPs can be conducted on individual critical infrastructure facilities or entire rail systems, with particular emphasis on critical control points.

In collaboration with the Transit Policing and Security Peer Advisory Group, formed under the auspices of the SCC, TSA works with transit agency managers and security professionals to harness the application of resources and the development of programs to maximize the impact in enhancing security. The Advisory Group brings together the expertise of 13 transit police chiefs and security directors from systems across the Nation as a sounding board and liaison group to advance effective security programs. Ongoing collaboration with these industry partners has facilitated assessment of transit systems' posture, notably in six Transit Security Fundamentals that are the core underpinnings to an effective transit security program. These efforts build on the work already accomplished in transit systems in assessing their security programs, whether through Federal technical assistance programs or contractual arrangements with private entities that conduct risk and vulnerability assessments.

The processes for normalizing, analyzing and prioritizing the results of security assessments and employing risk-based initiatives and protective programs to mitigate the identified risks are dynamic. Regular reviews and integration of information on the threat environment ensure these efforts remain properly focused and produce tools that may be employed effectively in the diverse public transportation environment. Such reviews also include the regular and on-going review of the effectiveness of Federal resources, programs and services. The goal of this plan, and the collaborative efforts and programs it addresses, is to ensure the most effective means to achieve more secure and better protected mass transit and passenger rail systems.

2 Mass Transit and Passenger Rail

2.1 Vision for the Mode

The Mass Transit Mode's vision is a secure, resilient transit system that leverages public awareness, technology, and layered security programs while maintaining the efficient flow of passengers and encouraging the expanded use of the Nation's transit services.

Since the attacks of September 11, the more recent attacks on transportation targets such as the 2005 London bombings, and the coordinated attack on four commuter trains in Madrid in 2004, the mass transit and passenger rail industry has made great strides in managing and mitigating risk and enhancing security of the systems. Many of the systems have prepared security and emergency plans, developed and implemented enhanced awareness and training programs for employees and the public, expanded emergency drills and exercises, improved their surveillance and detection capabilities, hardened and improved access control for critical assets and systems, and deployed various security enhancement technologies. Some have engaged in limited screening activities and deployed law enforcement surge teams, initiated or enhanced explosives detection canine programs, and participated in testing and development programs for emerging security technologies. As a whole, the mass transit and passenger rail industry has been alert, diligent and innovative in enhancing security of the employees and the traveling public.

The overall efforts of public and industry partners seek to develop capabilities for enhanced deterrence through visible/covert, random, and unpredictable security activities and engagement of security force multipliers by expansion of security training for mass transit and passenger rail system employees, drills and exercises, and public awareness campaigns.

TSA focuses particular attention on six Transit Security Fundamentals that provide the foundation for a successful security program. The fundamentals are:

1. Protection of high-risk underwater/underground assets and systems
2. Protection of other high-risk assets that have been identified through system-wide risk assessments
3. Use of visible, unpredictable deterrence
4. Targeted counter-terrorism training for key front-line staff
5. Emergency preparedness drills and exercises
6. Public awareness and preparedness campaigns

TSA and other components within DHS, in conjunction with Federal security partners at the Department of Transportation (DOT) to include the FTA and the FRA, the FBI, and State, local, tribal, and private sector partners, have also taken several steps to manage risk, expand mutual engagement, and strengthen our Nation's passenger rail and transit systems. Further, transit labor representatives have also taken significant steps to address security concerns in the industry, including producing and distributing their own security training videos and pamphlets, conducting joint labor-management conferences on transit security, working with DOT, TSA and industry security experts to develop Transit Watch (described in section 3.1.3), and contributing to the design, distribution and promotion of the National Transit Institute's security and emergency response training programs for frontline transit employees.

Enhancing transportation security requires a layered approach, integrating intelligence collection and analysis and law enforcement investigations to thwart plans before execution with the application of security resources and visible and random activities in ways that maximize deterrent effect. DHS, through its Office of Intelligence and Analysis, and the TSA, through its

Office of Intelligence (OI), integrate with the United States Intelligence Community to ensure continual situational awareness. These offices develop intelligence products and informational materials that inform the efforts of governmental decision makers and transit system operators and security officials. This concerted effort aims to track potential threats, disrupt their development, and focus Federal security resources and activities as necessary for detection, deterrence, and prevention.

An integrated public/private strategy for mass transit and passenger rail security, as with overall transportation security, is guided by five operating principles described below in Figure 2-1.

Figure 2-1: Operating Principles

Operating Principles
(1) Apply risk-based analysis in making investment and operational decisions
(2) Avoid giving terrorists or potential terrorists an advantage based on our predictability
(3) Intervene early based on intelligence and focus security measures on the terrorist, as well as the means for carrying out the threat
(4) Build and take advantage of security networks
(5) Invest in protective measures that would mitigate the impact of potential terrorist actions

The Transportation Sector-Specific Plan (TSSP) integrates Systems-Based Risk Management (SBRM) methodology which drives security initiatives, programs, and exercises to enhance operational capabilities and effectiveness. Mass Transit’s implementation of the TSSP leverages randomness and unpredictability, smart application of technological tools, and coordinated training and outreach efforts to stakeholders. A coordinated and cohesive implementation of this strategy can be achieved only through meaningful engagement of all Federal, State, local, and private sector partners.

2.2 Description of Mode

2.2.1 Overview

The Mass Transit and Passenger Rail mode includes service by buses, rail transit (commuter rail, heavy rail—also known as subways or metros—and light rail, including trolleys and streetcars), long-distance rail, namely Amtrak and Alaska Railroad, passenger ferryboats, and other, less common types of service (cable cars, inclined planes, funiculars and automated guideway systems). It also includes demand response services for seniors and persons with disabilities as well as vanpool/rideshare programs and taxi services operated under contract with a public transportation agency. Mass Transit and Passenger Rail mode does not include over-the-road motorcoach operators, school bus systems, and private shuttle system operators.

Approximately 6000 transit service providers, commuter railroads and long distance passenger railroad providers operate in the United States. The majority of these agencies operate more than one mode of service. About 2,000 agencies provide bus services; 5,300 agencies operate demand response services; and 150 agencies operate other forms of transportation such as inclined planes or water-borne services.¹ There are 565 transit systems that operate in urbanized areas of a population greater than 50,000 persons. Additionally, Amtrak operates the Nation’s primary intercity passenger rail service over a 22,000-mile network, primarily over leased freight railroad tracks. As part of an intermodal system of transportation, the mass transit and passenger rail mode also connects to other modes of transportation through multimodal systems and within multimodal infrastructures.

¹ FTA National Transit Database (NTD), <http://www.ntdprogram.com/ntdprogram/>

In 2006, Americans took 9.7 billion trips using mass transit and passenger rail. Since 1995, the ridership in the U.S. has grown by more than 23 percent, faster than highway travel. The American Public Transportation Association (APTA) estimates that about 33 million trips are taken each weekday in the United States. Heavy rail systems—subway systems like New York City’s transit system and Washington, DC’s Metro—typically operate in dedicated rights-of-way within a metropolitan area, draw electric power from a third rail and have the capacity for a heavy volume of traffic. Commuter rail systems, which often share operation on freight railroad tracks, consist of a diesel or electric-powered locomotive and a set of passenger rail cars and provide regional service (e.g., between a central city and adjacent suburbs). Light rail systems are typically characterized by lighter weight passenger rail cars, drawing electric power from overhead power lines, and often operate in shared-use rights-of-way, including streets with vehicular traffic.

Amtrak serves more than 500 stations (240 of which are staffed) in 46 states and the District of Columbia and carried more than 25 million passengers in 2004. According to Amtrak, about two-thirds of its ridership is concentrated in the “Northeast Corridor,” between Boston and Washington, D.C. Amtrak owns about 650 miles of track. Stations are owned by Amtrak, freight carriers, municipalities, and some private entities. Amtrak also operates commuter rail services in certain jurisdictions on behalf of State and regional transportation authorities.

Mass transit and passenger rail provide transportation that improves the quality of life in communities across the country by providing safe, efficient, and economical service. Some of the most significant benefits are listed in Figure 2-2.

Figure 2-2: Significant Benefits of Mass Transit

Significant Benefits of Mass Transit	
<ul style="list-style-type: none"> ▪ Easing Traffic Congestion ▪ Creating and Sustaining Jobs ▪ Providing Access to Jobs ▪ Stimulating Economic Development ▪ Boosting Real Estate Values ▪ Fostering More Livable Communities ▪ Providing Mobility for Seniors 	<ul style="list-style-type: none"> ▪ Providing Access for Rural Areas ▪ Improving Air Quality ▪ Reducing Energy Consumption ▪ Saving Money ▪ Enhancing Mobility During Emergencies ▪ Ensuring Safety

2.2.2 Responsibilities

Securing the Nation’s passenger rail and mass transit systems is a shared responsibility requiring coordinated action by Federal, State, and local governments, the public transportation agencies, their employees, and the passengers who ride these systems. Since the September 11 attacks, the role of the Federal Government in this area continues to evolve. Prior to September 11, DOT—namely, FTA and FRA—was the primary Federal entity involved in mass transit and passenger rail security matters. In response to the attacks of September 11, Congress enacted the Aviation and Transportation Security Act (ATSA), which created TSA within DOT and defined its primary responsibility as ensuring security in all modes of transportation. The Act also gave TSA regulatory authority and responsibility for security over all transportation modes. With the passage of the Homeland Security Act of 2002,² TSA was transferred, along with more than 20 other agencies, to DHS.

In executing its responsibilities and duties, TSA is specifically empowered to develop policies, strategies and plans for dealing with threats to transportation.³ As part of its security mission,

² Public Law 107-296

³ 49 U.S.C. 114(f)(3).

TSA is responsible for assessing intelligence and other information to identify individuals who pose a threat to transportation security and to coordinate countermeasures with other Federal agencies to address such threats.⁴ TSA also is to enforce security-related regulations and requirements,⁵ oversee the implementation and ensure the adequacy of security measures at transportation facilities,⁶ and carry out other appropriate duties relating to transportation security.⁷ TSA has broad regulatory authority to achieve ATSA's objectives, and may issue, rescind, and revise such regulations as are necessary to carry out TSA functions, including issuing regulations and security directives without notice or comment or prior approval of the Secretary of DHS if determined necessary to protect transportation security.⁸ TSA is also charged with serving as the primary liaison for transportation security to the intelligence and law enforcement communities.⁹

TSA's authority with respect to transportation security is comprehensive and supported with specific powers related to the development and enforcement of regulations, security directives, security plans, and other requirements. Accordingly, under this authority, TSA may identify a security threat to any mode of transportation, develop a measure for dealing with that threat, and enforce compliance with that measure.¹⁰

TSA has implemented its authority for mass transit and rail security in a number of ways. In the aftermath of the attacks on commuter trains in Madrid in March 2004, TSA issued two security directives applicable to passenger rail and rail transit. The directives, designated SD RAILPAX-04-01 and SD RAILPAX-04-02, mandate specific measures intended to enhance the security of the U.S. passenger rail and mass transit mode. The measures required by the directives support DHS' overarching goals to prevent, protect, respond, and restore. They have the force of regulations and remain valid and effective until revised or superseded by subsequent action by TSA.

FTA conducts a range of non-regulatory safety and security activities, including safety- and security-related training, research, technical assistance, and demonstration projects. In addition, FTA promotes safety and security through its grant-making authority. FTA provides financial assistance to public transportation agencies, in both formula-based and discretionary grants, to plan and develop new systems and operate, maintain, and improve existing systems. FTA stipulates conditions of grants, such as certain safety and security statutory and regulatory requirements, and may withhold funds for noncompliance. FTA annually awards more than \$3.5 billion in capital improvement grants. For formula-based grants, such as FTA's Section 5307 Program, transit agencies are required to spend 1 percent or more of their annual allocations on security-related projects, or certify that they do not need to do so (based on criteria such as adequate non-5307 funds being available for funding security needs or assessments indicating no deficiencies). For transit agencies in areas over 200,000 population only security-related capital projects are eligible to meet the 1 percent threshold. Transit agencies in areas under 200,000 in population can apply both capital and operating security expenses (such as the cost of security staffing) to meet the 1 percent threshold. Additionally, under the Safe, Affordable, Flexible, Efficient Transportation Equity Act – A Legacy for Users (SAFETEA-LU),¹¹ the definition of capital programs has been expanded to include security and

⁴ 49 U.S.C. 114(f)(1)-(5).

⁵ 49 U.S.C. 114(f)(7).

⁶ 49 U.S.C. 114(f)(11).

⁷ 49 U.S.C. 114(f)(15).

⁸ 49 U.S.C. 114(l).

⁹ 49 U.S.C. 114(f)(1) and (5).

¹⁰ 49 U.S.C. 114(f)(1) and (5).

¹¹ Public Law 109-59, August 10, 2005

emergency planning and training and exercises, thus providing more flexibility to larger transit agencies in meeting the 1 percent threshold.

FRA has regulatory authority for rail safety over commuter rail operators and Amtrak. It employs more than 400 rail inspectors that periodically monitor the implementation of safety and security plans at these systems.

State and local governments, mass transit and passenger rail operators, and private industry are also integral to the Nation's mass transit and passenger rail security efforts. State and local governments might own or operate a significant portion of the passenger rail system. Even when State and local governments are not owners and operators, they are directly affected by mass transit and passenger rail systems that operate within and through their jurisdictions. Consequently, the responsibility for responding to emergencies involving the mass transit and passenger rail infrastructure often falls to State and local governments. Mass transit and passenger rail operators, which can be public or private entities, are responsible for administering and managing related activities and services, including security. Passenger rail operators can directly provide the service or contract for all or part of the service. Although all levels of government are involved in mass transit and passenger rail security, the primary responsibility to implement the measures and activities to secure rests with the operators.

2.2.3 Risk to Mass Transit System

Between 1995 and June 2005, there were more than 250 terrorist attacks worldwide against rail targets, resulting in almost 900 deaths and more than 6,000 injuries.¹² These figures predate the London attacks of July 2005 and the Mumbai attacks of July 2006 and do not include the persons killed and injured in those incidents.

Mass transit and passenger rail systems carry a high number of passengers every day and are open and fully accessible. For example, on average, more than 306,000 customers use the BART rail system daily. Additionally, the Chicago Transit Authority's 1,190 rail rapid transit cars operate more than over seven routes and 222 miles of track, providing 500,000 customer trips each day serving 144 stations. Unlike air transport, no access control or seat assignment is generally applied. The wide geographical coverage of mass transit and passenger rail networks provide numerous options for access and getaway. Multiple stops and interchanges lead to high passenger turnover, which is difficult to monitor effectively. The disruption of an entire operation can confuse the public and lead to panic just as it curtails mobility. The extensive and worldwide media coverage that potential attacks can generate not only affects the image of public transport, but also discredits the Federal, State and local governments. In line with the logic of its perpetrators, a potential terrorist attack on public transportation systems can result in a large number of victims, thereby achieving its desired effect. The recent examples of the Mumbai, London, and Madrid bombings—all involving use of multiple IEDs—are tragic reminders of this reality.

The consequences of an attack depend on the type of attack and the form of transportation. In a mass transit bus with a capacity of about 65 passengers, an attack would be significant. Subway and passenger rail trains present even greater potential consequences because of the higher number of passengers and cars and the enhanced effects of attacks in confined space difficult to evacuate or access, such as underground tunnels. Underwater tunnels present even greater response and recovery challenges. The network of a subway system, with these tunnels as well as moving trains and ventilation shafts, can facilitate distribution of a chemical or biological agent throughout its facilities and, because of exterior vents and station egress point,

¹² RAND Corporation Data Base of Terrorism Incident (RAND-MIPT) <http://www.tkb.org/Home.jsp>

affect areas of a city. A terrorist can attack a subway system by releasing a chemical/biological weapon in a station, subway car, tunnel, or through a ventilation shaft. A transit bus explosion in a crowded highway tunnel could have dire consequences, as well.

Other threats of terrorist incidents involving a train include placing a vehicle bomb near a station or track and introducing an IED or a lower-yield explosive in a station, train, bus, or laying explosives on a track. Deploying conventional or improvised explosives will likely result in scores of casualties. Terrorists choose high-visibility targets with high casualty potentialities and opportunities for captivating images of fires, smoke, wrecked vehicles, and bloodied passengers. In addition to scores of deaths, a threat from a terrorist incident on a subway train resides in the damage to nearby critical infrastructure (e.g., flooding of a tunnel or damage to system infrastructure and neighboring facilities). Since subways are located at some of the lowest elevations in a city, an explosion in a tunnel could prove disastrous. Consequences of such attacks can result in severe economic disruption and can, particularly in the example of the nation's capital, impact the governmental continuity of operations.

2.3 Transit, Commuter and Long-Distance Rail Government Coordinating Council and Sector Coordinating Council Structure and Process

The Transit, Commuter and Long-Distance Rail GCC (TCLDR-GCC) was established in March 2006. Members of the TCLDR-GCC include TSA, DHS, DOT, DOJ, and when appropriate, Department of Defense (DOD). Appropriate State and local representation is also being coordinated. Outreach to stakeholders in the mass transit and passenger rail community encouraged establishing of a modal coordinating council for the mass transit and passenger rail mode. With APTA acting as the Secretary to the Council, the Mass Transit SCC has been organized around an existing body of the APTA Security Affairs Steering Committee. Representing corporate and employee interests, participating entities include APTA, the Community Transportation Association of America (CTAA), Amalgamated Transit Union (ATU), Amtrak, and individual transit agencies representative of the community in system size and geographic spread, as well as representation of business organizations providing support services the public transportation industry. Additions may be made to this group to ensure a more robust and broad private sector engagement. Both the TCLDR-GCC and the Mass Transit SCC commit to ensuring that the status of their respective members ensures their capability to effect decisions as may be required.

One of earliest and most important joint tasks of the TCLDR-GCC and Mass Transit SCC is to implement the TSSP and the plan outlined in this annex. This effort is occurring under the Critical Infrastructure Partnership Advisory Council (CIPAC) umbrella through a cooperative effort that will be tailored to the particular circumstances best suited for the conditions under which the activity will be conducted. The TSA's Mass Transit Division prepared a preliminary draft and shared it with other TSA entities and members of the TCLDR-GCC and SCC. TCLDR-GCC and SCC comments and changes were then incorporated into the draft Plan. The responsibilities of GCC and SCC extend to other important areas/efforts as well, such as support of APTA's Security Standards Development Program, all of which rely upon efficient information-sharing capabilities and effective and timely policy determinations.

Transportation security strategic policy is being developed through the GCC/SCC and the CIPAC process. These efforts will be initially coordinated at the modal level and recommendations will be made to senior government leadership through the Transportation Sector GCC. The government maintains the prerogative of developing necessary policy, especially in response to specific and immediate threats.

3 Implementation Plan

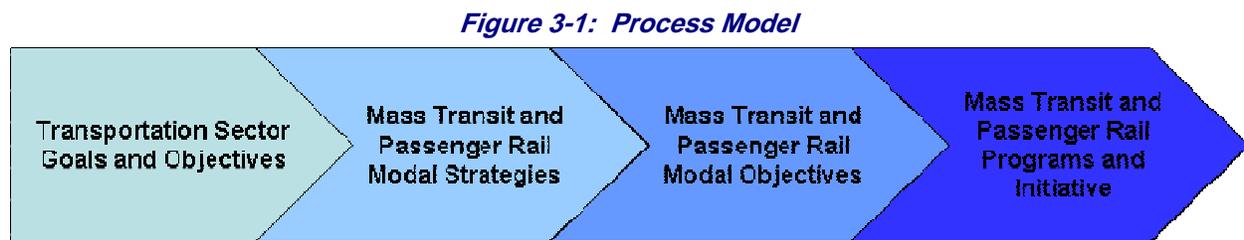
3.1 Goals, Objectives, and Programs/Processes

The TSSP identifies a set of goals and objectives for the transportation sector. Achieving these goals and objectives requires a strategic approach that integrates the needs and requirements of the private sector through a meaningful collaboration between public and private partners. To that end, mass transit and passenger rail security partners have worked together to devise a plan that includes priorities and programs that are aligned with the TSSP goals and objectives and employ risk-informed decision making to determine specific actions.

The plan to enhance security in mass transit and passenger rail is focused on:

- ❑ Expanding partnerships for security enhancement;
- ❑ Continuously advancing the security baseline;
- ❑ Building security force multipliers;
- ❑ Security information leadership; and
- ❑ Deploying tools to mitigate high consequence risk.

Figure 3-1 below demonstrates the process model culminating in mass transit and passenger rail security programs and initiatives.



The TSSP goals of (1) preventing and deterring acts of terrorism using or against the U.S. transportation system, (2) enhancing resiliency of the U.S. transportation system, and (3) improving the cost-effective use of resources for transportation security.

3.1.1 Expanding Partnerships for Security Enhancement

A close partnership with appropriate parties is paramount to enhancing the security of mass transit and passenger rail and an integral element of the overall strategy. As discussed above, we are furthering this strategy through constructive engagement with governmental security partners via the TCLDR-GCC and transit system operating and security officials via the Mass Transit SCC and the Transit Policing and Security Peer Advisory Group; and regional collaboration through encouragement of regional coordinating councils.

Additionally, through regional engagement and regional deployment of resources, we are enabling the use of a full spectrum of available resources from Federal, State, and local governmental entities and the area transit systems which aims to disrupt the terrorists' ability to orient planning and preparation activities. This regional deployment approach entails developing and implementing a sustainable program to elevate security posture through visible and random deterrent activities and to enhance vigilance through security training and awareness programs. The Federal security teams coordinate with transit and passenger rail agencies in advance to effectively integrate with local resources targeted force packages to enhance security. These

teams, consisting of the STSIs, Federal Air Marshals (FAM), explosive detection canine teams, and others, help expand application of visible, random, unpredictable security activities throughout the transit and passenger rail system, and set the foundation for sustained collaboration through existing surface transportation coordinating committees or regional GCC/SCC structure. Federal resources will be deployed in a manner that is consistent with the operational environments of transit services.

3.1.2 Continuously Advancing the Security Baseline

Establishing security guidelines and action items to help elevate the security baseline and posture is a major priority for mass transit and passenger rail security. TSA and FTA recently finalized a collaborative effort, coordinated with the Mass Transit SCC for review and input, to update the 20 action items FTA developed in the aftermath of September 11. The new action items for transit agencies represent a comprehensive update addressing the new security threats and risks that confront transit agencies today, and priority areas with gaps in security and emergency preparedness programs. The security action items and the six transit security fundamentals support achievement of the goals and objectives articulated in the NIPP and the TSSP, and the mandates of the Presidential Executive Order on surface transportation. The STSI Program, through inspections, assessments, and technical assistance, together with the systems' self-assessments, and other efforts by governmental and industry partners discussed throughout this plan, advance security baselines and enhance security posture throughout the passenger rail and mass transit mode.

3.1.3 Building Security Force Multipliers

We are building security force multipliers through security training for front-line employees, including vehicle operators, maintenance employees and customer service personnel, drills and exercises, public awareness campaigns, and outreach and resource deployment to encourage expanded employment of visible, random security activities; bolstered by regional collaboration to ensure the broadest application of the available security resources in the most effective means. Public awareness and improved training programs are a key component of this approach. New training initiatives are needed to address the non-traditional terrorist threats (e.g., chemical, biological, and improvised explosive devices) to mass transit and passenger rail systems. The personnel working for these systems nationwide are the driving force behind any successes relating to transportation system security. Therefore, as the foundation for technological and procedural initiatives, security awareness training is the essential component to enhanced effectiveness in preventing terrorist attacks on the rail systems. Mass Transit and passenger rail employee training is one of the security priorities of the NIPP and directly supports the National Priorities, the National Preparedness Goal, and the NSTS.

Since September 11, mass transit and passenger rail agencies have developed and implemented public awareness materials that are both general and specific with their message. More recently, public awareness campaigns have expanded to include a focus specifically on unattended bags and emergency evacuation procedures. The Federal Government has partnered with the industry and labor representatives in several public awareness efforts, as explained in the Programs/Process Section of this annex. For example, TSA partners with FTA in Transit Watch, a program focused on developing and widely disseminating public awareness materials that mass transit and passenger rail agencies may adapt for their particular circumstances and use throughout their systems. Two particularly successful Transit Watch campaigns have been "Is this your Bag?" and the "See Something? Say Something!" messages which remind mass transit riders to report suspicious bags or behavior, thereby empowering riders to become the "eyes and ears" of mass transit.

TSA, FTA and OGT have established an interagency training development and review committee pursuant to the Public Transportation Security Annex to the DOT/DHS Memorandum of Understanding (MOU) executed September 2004. (See section 3.2 for a discussion of this MOU annex.) This group is being developed into a broader GCC/SCC working group to focus on the developing of training initiatives for the mass transit industry. The group will evaluate and update existing training material, determine additional training requirements, coordinate with the transit community, advance the development of new initiatives based on the needs of the transit community, and identify and apply appropriate funding.

3.1.4 Security Information Leadership

A robust information strategy is central to a successful approach to securing our Nation's mass transit and passenger rail systems. This strategy focuses on the capability to collect, analyze, integrate, and disseminate to decision makers for action an uninterrupted flow of information while exploiting or denying a terrorist's ability to do the same. This approach enables informed decisions, timely application of resources, and effective implementation of security activities for detection, deterrence, and prevention of terrorist attacks and for response and recovery from such attacks, should they occur. At the same time, it disrupts and denies potential terrorists the ability to plan and orient their activities effectively with the purpose of undercutting attack preparations and minimizing the consequences should an attack occur.

Information assurance and information operations encompass the means employed to achieve this strategic objective. Information assurance protects information processes and information systems to ensure the availability, integrity, authenticity, accuracy, and, where appropriate, confidentiality of relevant information while denying terrorists the ability to exploit, disrupt, or deny these advantages. Information operations target the eyes, ears, and minds of potential terrorists, specifically seeking to disrupt the ability to observe and orient planning and preparation activities and to make the decision to conduct an attack.

The information strategy for mass transit and passenger rail security advances key objectives of the broader homeland security strategic agenda. Consistent with HSPD-5, *Management of Domestic Incidents*, this strategy implements a network approach to government security efforts that overcomes bureaucratic stove piping and ensures the capability of Federal agencies to work together efficiently and effectively. Through the modal and regional GCC, Federal, State, and local governmental entities with security responsibilities collaborate in strategic and operational planning, training, exercises, and employ resources to maximum effect. Similar collaborative efforts with the modal and regional SCCs promote partnerships across the spectrum of security activities, including incident management. By maintaining the flow of timely, accurate, and relevant information on mass transit and passenger rail security, the strategy supports the National Incident Management System and executes of the National Response Plan.

The strategy depends upon and affects the public-private partnership. Operating through the GCC/SCC framework, the information strategy establishes security networks integrating governmental partners at the Federal, State, and local levels and public transportation stakeholders. The CIPAC process affords the opportunity for a consensus-based engagement between GCC and SCC members to enhance security through the identifying strategic priorities and developing and implementing of security strategies, policies, and protective measures. This construct enables collaborative partnerships to leverage and maximize the impact of available security resources.

Finally, the comprehensive information strategy meets six of the seven security priorities identified in HSPD-8, *National Preparedness*. The strategic objective of information dominance

supports the National Incident Management System and execution of the National Response Plan. Close collaboration among governmental entities and with public transportation stakeholders through the GCC/SCC framework and CIPAC process implements the NIPP. Extending these forums by emphasizing the establishment of regional GCCs and SCCs expands regional collaboration across the mode and the transportation sector. These collaborative efforts focus specifically on strengthening information-sharing, interoperable communications, and detection, response, and disposal or decontamination of IEDs, including those with chemical, biological, radiological, or nuclear capability.

3.1.5 Deploying Tools to Mitigate High Consequence Risks

Technology, in conjunction with training, public awareness initiatives, exercises, and effective practices, is an essential part of a comprehensive strategy to mitigate high consequence risk. Technology can provide transit personnel and first responders critical information to prevent, detect, and deter a terrorist attack in their system, as well as aid with continuity of operations during incidents or threats. The mass transit and passenger rail industry uses a variety of technologies to enhance the security of the systems. For many mass transit and passenger rail agencies, security technology is integrated into their daily operations.

Many transit systems across the U.S. are attempting to add increased technology to their layered security approach. Some examples include transit agencies' investment of millions of dollars in surveillance and intrusion detection technology throughout their system; satellite based systems for bus tracking; and the testing of on-board cameras that can wirelessly transmit live color images.

Technology must be fully incorporated into the security operations of mass transit and passenger rail agencies. Presently, a variety of technologies are on the market or being tested, such as intrusion detection, video surveillance, anomaly detection, and chemical/biological/radiological/nuclear detection. TSA, along with its public and private partners, is working to identify technology gaps and conduct research and development to provide technological solutions. This process between government and industry will aid in ensuring that a collaborative strategic process for technology research, development and deployment is maintained. The Federal partners are also harnessing the information gained from completed developmental testing and other use experience to provide the transit community a security technology information resource to guide procurement decisions. This resource will be a key component of the Public Transit Portal in the HSIN, meeting a specific requirement of Executive Order 13416, "Strengthening Surface Transportation Security."

DHS is testing a number of technologies, which could be implemented or deployed quickly to systems facing a specific threat or in support of major events such as National Security Special Events (NSSEs). Pilots and studies are also underway in major American cities involving smart surveillance systems, emerging technologies in anomaly detection, vehicle disabling, passenger screening, and other areas. The PROTECT system is an example of technology that originated as a pilot program designed to detect a chemical attack. This program is now fully operational, integrating advanced chemical detection equipment and camera networks. The system also links with local emergency response assets to improve response time and capability. The system is currently deployed in segments of the Washington, DC, New York City, and Boston rail systems. The determination of transit industry technology needs and technologies to test is effected through a coordinated approach led by DHS in partnership with the mass transit and passenger rail industry.

3.1.6 Mass Transit Objectives

The key strategies above are the foundation for the specific modal objectives developed to enhance security in Mass Transit and Passenger Rail. The objectives, described in figure 3-2 below, are designed to take us one step closer to achieving enhanced security by providing flexibly applicable, mobile and fixed technological means to facilitate the process.

Figure 3-2: Mass Transit Objectives

Mass Transit Objectives
<ul style="list-style-type: none"> ▪ Employ technology for screening passengers and bags in random applications throughout the mass transit and passenger rail systems as appropriate.
<ul style="list-style-type: none"> ▪ Bolster screening technology efforts with a program for random searches of passengers' bags entering system.
<ul style="list-style-type: none"> ▪ Effect regional approach through coordinated planning among Federal regional officials (FSD, FAMSAC, STSI Program, Explosives Detection Canine teams, FBI), and State and local law enforcement, and transit system security officials to maximize application of available security resources through multiple teams for random, unpredictable activities throughout system.
<ul style="list-style-type: none"> ▪ Conduct Security Readiness Assessments through collaborative efforts between area Surface Transportation Security Inspectors and transit security officials to conduct security assessments under the TSA SAAP and the BASE.
<ul style="list-style-type: none"> ▪ Coordinate with system security officials to examine the capabilities of transit agencies and front-line employees in identifying and reporting suspicious items and activities. ▪ Entails setting unattended packages or staging other suspicious activities within the system to test awareness and reporting by employees and passengers.
<ul style="list-style-type: none"> ▪ Improve Intelligence and Security Outreach through coordination between TSA OI, and Transportation Sector Network Management (TSNM) Mass Transit, STSIs and the regional intelligence and information-sharing centers to implement through regional engagement.
<ul style="list-style-type: none"> ▪ Coordinate focused transit system employee training; TSA and FTA lead. ▪ Align program with needs and requirements of passenger rail or mass transit security officials. ▪ Sustain training emphasis through continuing regional engagement and coordination by field presence – Regional Directors of STSI Program and FTA regional officials.
<ul style="list-style-type: none"> ▪ Employ all available media—public address system announcements, billboards and posters, brochures, and reminding keepsakes, such as the key chain flashlights disseminated by TSA in the WMATA system. ▪ Use varying messages and multiple media to engage and retain public interest. ▪ Integrate TSA materials in joint program.

3.2 Security Programs and Processes

In September 2005, DHS and DOT executed an annex on public transportation to the MOU discussed in subsection 3.1.3. Within DHS, the agencies with primary responsibility for carrying out this annex are OGT and TSA, and within DOT, FTA and the Office of Intelligence, Security and Emergency Response (S-60) within the Office of the Secretary (OST). The annex stipulates that the parties have a mutual interest in ensuring coordinated, consistent, and effective activities that have the potential to materially affect the missions of both departments and sets out to delineate clear lines of authority and responsibility between the parties for transit security.

Pursuant to this annex, DOT and DHS agreed to coordinate their programs and services (including risk assessments, grants, training, exercises and technical assistance) to better assist transit agencies in prioritizing and addressing their current and emerging security-related needs. The areas of coordination identified in the annex include training courses; awareness programs, i.e.,

Working Groups
Assessments and Technical Assistance
Standards/Research
Transit Watch/Connecting Communities
Safety and Security Roundtables
National Resource Center
Training
Annual Plan/RTSS/Grants
Emergency Drills/Exercises

the Transit Watch; forums to encourage and facilitate communications and information-sharing, i.e. the Safety and Security Roundtables; drills and exercises; emergency preparedness and security forums, i.e., Connecting Communities; creating a comprehensive source for transit system officials to turn for information about available Federal security and preparedness resources (e.g., information on grant funding availability, training, technical assistance, and effective practices), risk assessment and security reviews, and interoperable communication.

In support of the MOU annex implementation, eight working groups have been established under an Executive Steering Committee consisting of DHS/OGT, DHS/TSA and DOT/FTA. Several of these working groups are in the process of being integrated into the TCLDR-GCC and SCC under the CIPAC process.

In addition to the areas identified in the MOU, the Federal Government and its public and private partners, have initiated a set of mass transit and passenger rail programs and processes that are designed to enhance security in the mode and advance the overall strategic approach. The following represents these programs and processes, some of which carry out the priorities for cooperation identified in the MOU. These programs and process are aligned with overall TSSP goals and objectives and each helps achieve a specific goal and its corresponding objective(s). Figure 3-3 demonstrates this connection.

Figure 3-3: Security Programs/Goals/Objectives

Programs	Goals	Objectives
Surface Transportation Security Inspection (STSI) Program	Goal 1: Prevent and deter acts of terrorism using or against the transportation system	Objective B: Increase vigilance of travelers and transportation workers (e.g., through security awareness information) Objective C: Enhance information and intelligence sharing among transportation sector security partners (e.g., Federal, State, local and tribal government, the private sector and international security partners)
	Goal 2: Enhance resiliency of the U.S. transportation system	Objective A: Assess, manage, and reduce the risk associated with key nodes, links, and flows within critical transportation systems (e.g., robustness, redundancy, and technology)
	Goal 3: Improve the cost-effective use of resources for transportation security	Objective A: Align sector resources with the highest priority transportation security risks using both risk and economic consequences as decision criteria
Explosives Detection Canine Teams	Goal 1: Prevent and deter acts of terrorism using or against the transportation system	Objective A: Implement risk-based, flexible, layered, and unpredictable security programs Objective B: Increase vigilance of travelers and transportation workers (e.g., through security awareness information)

**Explosives Detection
Canine Teams**

Programs	Goals	Objectives
	Goal 2: Enhance resiliency of the U.S. transportation system	Objective A: Assess, manage, and reduce the risk associated with key nodes, links, and flows within critical transportation systems (e.g., robustness, redundancy, and technology)
	Goal 3: Improve the cost effective use of resources for transportation security	Objective A: Align sector resources with the highest priority transportation security risks using both risk and economic consequences as decision criteria Objective B: Maximize sector participation as a partner in the developing and implementing of public sector programs for Critical Infrastructure/Key Resource protection
Visible Intermodal Prevention and Response (VIPR) teams.	Goal 1: Prevent and deter acts of terrorism using or against the transportation system	Objective A: Implement risk-based, flexible, layered, and unpredictable security programs Objective B: Increase vigilance of travelers and transportation workers (e.g., through security awareness information) Objective C: Enhance information and intelligence sharing among transportation sector security partners (e.g., Federal, State, local tribal government, the private sector, and international security partners)
	Goal 2: Enhance Resiliency of the U.S. transportation system	Objective A: Assess, manage, and reduce the risk associated with key nodes, links, and flows within critical transportation systems (e.g., robustness, redundancy, and technology)
Information Sharing: <ul style="list-style-type: none"> ▪ Mass Transit and Passenger Rail Information Sharing Network ▪ National Resource Center 	Goal 1: Prevent and deter acts of terrorism using or against the transportation system	Objective C: Enhance information and intelligence sharing among transportation sector security partners (e.g., Federal, State, local tribal government, the private sector, and international security partners)

Programs	Goals	Objectives
Security Training and Awareness Programs: <ul style="list-style-type: none"> ▪ Connecting Communities ▪ Safety and Security Roundtables ▪ FLTEC- Land Transportation Anti-Terrorism Training ▪ Transit Watch ▪ Interactive Computer-Based Training for Railroad Employees ▪ Random High-Visibility Passenger Awareness 	Goal 1: Prevent and deter acts of terrorism using or against the transportation system	Objective B: Increase vigilance of travelers and transportation workers (e.g., through security awareness information)
	Goal 2: Enhance Resiliency of the U.S. transportation system and perform collaborative risk analysis processes.	Objective B: Ensure the capacity for rapid response and recovery to all-hazards events (e.g., flexibility, timeliness, etc)
	Goal 3: Improve the cost effective use of resources for transportation security	Objective C: Improve transportation sector security research, development, test, and evaluation resource allocation (e.g., leveraging technology expertise, minimizing redundancies)
National Tunnel Security Initiative	Goal 1: Prevent and deter acts of terrorism using or against the transportation system	Objective A: Implement risk-based, flexible, layered, and unpredictable security programs Objective C: Enhance information and intelligence sharing among transportation sector security partners (e.g., Federal, State, local tribal government, the private sector, and international security partners)
	Goal 2: Enhance resiliency of the U.S. transportation system	Objective A: Assess, manage, and reduce the risk associated with key nodes, links, and flows within critical transportation systems (e.g., robustness, redundancy, and technology) Objective C: Develop, disseminate, and promote the adoption of a standard risk reduction methodology
	Goal 3: Improve the cost effective use of resources for transportation security	Objective A: Align sector resources with the highest priority transportation security risks using both risk and economic consequences as decision criteria Objective B: Maximize sector participation as a partner in the developing and implementing of public sector programs for Critical Infrastructure/Key Resource protection Objective C: Improve transportation sector security research, development, test, and evaluation resource allocation (e.g., leveraging technology expertise, minimizing redundancies) Objective D: Ensure that public sector funds expended have achieved the expected risk reduction
Security Technology Deployment	Goal 1: Prevent and deter acts of terrorism using or against the transportation system	Objective A: Implement risk-based, flexible, layered, and unpredictable security programs Objective B: Increase vigilance of travelers and transportation workers (e.g., through security awareness information)
	Goal 2: Enhance resiliency of the U.S. transportation system	Objective A: Assess, manage, and reduce the risk associated with key nodes, links, and flows within critical transportation systems (e.g., robustness, redundancy, and technology)
	Goal 3: Improve the cost effective use of resources for transportation security	Objective A: Align sector resources with the highest priority transportation security risks using both risk and economic consequences as decision criteria Objective B: Maximize sector participation as a partner in the developing and implementing of public sector programs for Critical Infrastructure/Key Resource protection Objective C: Improve transportation sector security research, development, test, and evaluation resource allocation (e.g., leveraging technology expertise, minimizing redundancies)

Programs	Goals	Objectives
Technology Research and Development	Goal 1: Prevent and deter acts of terrorism using or against the transportation system	Objective A: Implement risk-based, flexible, layered, and unpredictable security programs Objective B: Increase vigilance of travelers and transportation workers (e.g., through security awareness information)
	Goal 3: Improve the cost effective use of resources for transportation security	Objective C: Improve transportation sector security research, development, test, and evaluation resource allocation (e.g., leveraging technology expertise, minimizing redundancies)
International Initiatives	Goal 1: Prevent and deter acts of terrorism using or against the transportation system	Objective C: Enhance information and intelligence sharing among transportation sector security partners (e.g., Federal, State, local tribal government, the private sector, and international security partners)
	Goal 2: Enhance resiliency of the U.S. transportation system	Objective B: Ensure the capacity for rapid response and recovery to all-hazards events (e.g., flexibility, timeliness, etc.)

3.2.1 Surface Transportation Security Inspection (STSI) Program

The Department of Homeland Security Appropriations Acts for 2005 and 2006 allocated funds for the hiring and deploying “Federal rail compliance inspectors” (2005) and “rail inspectors” (2006). TSA created the STSI Program and deployed 100 rail inspectors to 19 field offices throughout the United States covering key rail and mass transit facilities throughout the regions. The program focuses on nationwide outreach and liaison activities with the rail industry and initiatives to enhance security in passenger rail and mass transit systems. These efforts include assessment programs specifically intended to expand TSA’s domain awareness, elevate the security baseline throughout the mode, and assist systems in identifying and mitigating security vulnerabilities.

STSI Field activities assess compliance with security requirements and implementation of noncompulsory security standards and protective measures with the objective of a broad-based enhancement of passenger rail and rail transit security. Through the Baseline Assessment and Security Enhancement (BASE) program, inspectors review the implementation by mass transit and passenger rail systems of the 17 security action items jointly developed by TSA, FTA, and the Mass Transit SCC. The security action items represent a comprehensive update of the Top 20 Security Program Actions for Mass Transit Agencies FTA developed in the aftermath of 9/11. This initiative aims to elevate security posture and readiness throughout the mass transit and passenger rail mode by implementing and sustaining baseline security measures applicable to the operating environment and characteristics of mass transit and passenger rail systems.

Additionally, the TSA surface inspectors are actively engaged in performing Security Analysis and Action Program (SAAP) assessments, which constitute a systematic examination of stakeholders’ operations to assess compliance with security requirements, identify security gaps, develop effective practices for sharing across the mode, and gathering baseline information on the system, its operations, and its security resources and initiatives. The program utilizes several different tools to identify vulnerabilities based on specific scenarios, such as an IED on a passenger train. SAAPs can be conducted on individual critical infrastructure facilities or entire rail systems, with particular emphasis on critical control points. As a component of

these evaluations, TSA focuses particular attention on six Transit Security Fundamentals, explained in section 3.4, that provide the essential foundation for a successful security program.

In a cooperative effort with the FTA, the STSI Program offers assistance to State Safety Oversight Agencies (SSOA) in completing security audits of the Nation's 26 rail transit systems under 49 CFR Part 659, *Rail Fixed Guideway Systems; State Safety Oversight*¹³. This regulation, administered by FTA, requires rail fixed guideway¹⁴ systems not regulated by FRA as a railroad to maintain a system security plan that meets specific parameters, to conduct annual reviews of the plan, and to conduct internal security reviews of the implementation and effectiveness of the security plan. The oversight agencies must ensure transit systems under their responsibility conduct an annual review of their system security program plan.¹⁵ Additionally, the oversight agencies must develop and document a process for conducting ongoing assessments of implementation of the system security program plan.¹⁶ Covered rail transit systems must complete these assessments of all required elements of their system security program plan over a 3-year cycle. Each State Safety Oversight Agency (SSOA) is required to perform an on-site review of implementation of the system security program plan at least every 3 years.¹⁷

The STSI Program is providing security assistance and integrating its broader security assessments in a comprehensive approach that limits disruptions to transit system operations and "audit fatigue." In conjunction with FTA, TSA has initiated coordinated security review and audit activities with the SSOAs. TSA STSI Program representatives participated in the SSOA Directors' meeting in St Louis in June 2006 and a planning and strategy session occurred with California Public Utilities Commission officials during June 21-22 in San Francisco. STSIs conducted the first combined SSOA security review and TSA security assessment at the BART system in San Francisco/Oakland in August 2006. TSA representatives attended the annual SSOA meeting in Salt Lake City in September 2006, joining FTA officials in explaining the benefits of the combined approach.

Combined SSOA audits and BASE reviews are occurring in heavy rail transit systems covered by 49 CFR Part 659. In August 2006 with audits of the Bay Area Rapid Transit (BART) rail system in San Francisco, the Newark subway in the New Jersey Transit system, and the Port Authority Transit Corporation (PATCO) rail system serving commuters between southwestern New Jersey and the Philadelphia area.

The SSOAs have responded positively to this outreach. In most cases, they seek assistance on the security component of their responsibilities and welcome the opportunity to work with TSA inspectors. The joint efforts will also minimize disruptions to transit system operations and enable TSA inspectors to review other aspects of transit systems' compliance with security requirements, standards, and recommended measures and practices.

Finally, TSA deploys STSI inspectors to serve as Federal liaisons to mass transit and passenger rail system operations centers and provide other security support and assistance in periods of heightened threat or in response to security incidents. TSA initiated this component of STSI Program responsibilities in the aftermath of the attacks on the London transit system in July 2005. TSA inspectors deployed to the operations centers of the transit systems in their areas to assess the security response and serve as liaison for information and coordination of

¹³ 49 CFR § 659

¹⁴ 49 CFR § 659.5, Fixed Guideway Systems; State Safety Oversight Rail, defines fixed guideway systems as any light, heavy, or rapid rail system, monorail, inclined plane, funicular, trolley, or automated guideway.

¹⁵ See 49 CFR § 659.25

¹⁶ See 49 CFR § 659.27

¹⁷ See 49 CFR § 659.29

resource support from the Federal Government. Since this initial deployment, inspectors have developed relationships with security officials in transit systems in their areas, coordinated access to operations centers, participated in or observed exercises, and provided other assistance consistent with the overall objective of enhancing security through collective effort.

3.2.2 National Explosives Detection Canine Teams

Since late 2005, TSA’s National Explosive Detection Canine Team Program (NEDCTP) has worked in partnership with mass transit systems to train, certify, and deploy 56 explosives detection canine teams to 13 major systems in a risk-based application of resources. Forty-two of these teams are currently online and the other 14 are projected for training, certification, and deployment by the end of FY 2007. This outreach will continue as an effective means by which TSA provides security enhancement resources to mass transit and passenger rail systems. The initial 14 systems integrated into this program are listed in figure 3-4 below.

Figure 3-4: The Initial 13 Systems Selected to Participate in NEDCTP

System Participation in NEDCTP	
<ul style="list-style-type: none"> ▪ Massachusetts Bay Transportation Authority (MBTA) ▪ San Francisco Bay Area Rapid Transit District (BART) ▪ Southeastern Pennsylvania Transportation Authority (SEPTA) ▪ Washington Metropolitan Area Transit Authority (WMATA) ▪ Port Authority Trans-Hudson Corporation (PATH) ▪ Dallas Rapid Area Transit (DART) ▪ Tri-County Metropolitan Transportation District of Oregon (TriMet) 	<ul style="list-style-type: none"> ▪ Chicago Transit Authority (CTA) ▪ Los Angeles County Metropolitan Transportation Authority (Metro) ▪ Maryland Transit Administration (MTA) ▪ San Francisco Municipal Railway (Muni) ▪ San Diego Trolley, Inc. (SDTI) ▪ Metropolitan Atlanta Rapid Transit Authority (MARTA)

The TSA-trained and certified explosive detection canine teams provide a visible and effective detection and deterrence presence in the public transportation system and can be surged to other venues as threats dictate. They can post at key junctions or points within systems, stations, terminals, and facilities, and deploy throughout rail systems. Random employment heightens the deterrent effect.

For the deployment initiative in mass transit, TSA provides the canine training for the handler and the dog, and system orientation on completion of the training and certification program. TSA also allocates funds to cover the initial costs associated with continuing training and maintenance of the capabilities of the team. The transit system commits a handler to attend the TSA training and certification program.

As part of its training facility in San Antonio, TSA has established a training lab specifically for mass transit canine training that will include rail cars. Through a partnership with the FRA, the NEDCTP has obtained two rail cars at no cost to use as canine training aids. As a result of newly acquired classroom space along with additional training staff, the TSA Canine Support Branch now has the ability to train 108 new canine teams during each calendar year.

An additional, critical mission of the NEDCTP is the deploying of TSA-trained and certified teams to provide security support during National Security Special Events. This resource also enables deployment of teams in periods of heightened threats and in response to specific threats or security incidents. As one example, in response to the attacks on transit systems in London and Madrid, TSA deployed teams to enhance security in transit systems throughout the U.S.

3.2.3 Visible Intermodal Prevention and Response (VIPR) Teams

As part of implementing flexible, layered, and unpredictable security programs using risk management principles, this TSA program trains various teams including law enforcement

personnel, canine teams, and inspection personnel for deployment to supplement mass transit and passenger rail system efforts to deter and protect against potential terrorist actions. The Visible Intermodal Prevention and Response (VIPR) teams provide TSA and the transit and passenger rail agencies with the ability to leverage a variety of resources quickly and effectively. Consisting of FAMs, STSIs, TSA-certified explosive detection canine teams, and advanced screening technology, VIPR teams represent an ongoing effort to develop surge capacity to enhance security in public transportation systems. The teams work with local security and law enforcement officials to supplement existing security resources, provide deterrent presence and detection capabilities, and introduce an element of unpredictability to disrupt potential terrorist planning activities. These deployments enhance the agency's ability to leverage a variety of resources to raise the level of security quickly and effectively. By engaging regional, State, and local law enforcement and security entities as part of the VIPR teams, this program ensures robust sector participation.

Nearly 50 VIPR exercises have been conducted at various mass transit and passenger rail systems throughout the Nation since the program initiated in December 2005 (as of March 20, 2007). TSA has directed and managed these exercises at the national level. Consistent with the mass transit and passenger rail regional deployment strategic plan, the planning for VIPR team deployment will continue in 2007 at the national level simultaneously with regional planning and deployment of the teams integrating their deployment with other available regional, State and local resources. Regional application of this program to facilitate more frequent deployments and exercises enhances deterrent effect. Continued oversight at the national level will advance the development of surge capacity and ensures effective employment of TSA security resources.

Mass Transit Resource Center

TSA is working with DHS/OGT and DOT/FTA to develop the Mass Transit Resource Center, the application of the NRC in the Public Transit Portal of HSIN. The Resource Center provides a comprehensive database for the transit industry to access information on a broad spectrum of subjects pertinent to transit security, material not readily available in a consolidated format elsewhere. TSA uses the Portal to provide timely security alerts, advisories, and information bulletins to passenger rail and mass transit agencies. Technology updates constitute an important component of this resource. Overall, the Resource Center covers more than 20 subjects areas of security interest to the public transportation community, reflecting the feedback received from stakeholders on the type of information they require to meet the security mission. The STSIs, through their various assessment programs such as BASE and SAAP reviews, provide information on smart security practices for sharing among all passenger rail and mass transit systems. Additionally, TSA's Mass Transit Division will prepare and coordinate through the interagency Mass Transit and Passenger Rail Security Information Sharing Network and the TCLDR-GCC a periodic newsletter providing items on Federal transit security initiatives, recent suspicious activity reporting with security context, and updates on model security practices observed in STSI assessments, technology programs, and other areas of interest. This effort will also incorporate effective practices and items of general interest from transit agencies. Private sector input and feedback will be vital in shaping this resource to meet industry needs.

3.2.4 Information-Sharing

Mass Transit and Passenger Rail Security Information Sharing Network

Effective information-sharing is paramount to achieving the TSSP goals and objectives. A streamlined and effective system to share mass transit and passenger rail information is needed

to facilitate information-sharing among subject matter experts in the Federal Government and with public and private stakeholders. More efficient and timely information-sharing will improve domain and situational awareness and allow the collaborative development of an agreed-upon common picture that Federal leadership can use to make well-informed and timely decisions.

In February, 2002, the FTA provided grant support to APTA to establish the Public Transit ISAC (PT-ISAC) which is a 24 hour/7 day a week information-sharing analysis center supported by analysts who cull through secure and open sources and communicate security-related information and advisories to public transit systems. Currently over 400 transit systems participate in the PT-ISAC. The ISAC has both a website analyst support and an electronic mail capability that can be used to share information with a broader audience. Somewhat similar is the DHS/TSA and other agency communication tools (DOT – Crisis Management Center (CMC)) capability to use electronic e-mail to pass along sensitive and non-sensitive information to stakeholders. All of these capabilities are important to maintaining a robust series of networks for sharing of information between the government and industry.

In August 2005, TSA initiated the interagency Passenger Rail and Rail Transit Information Pilot to bring together Federal partners to develop processes for information-sharing and communications protocols, to eliminate duplication of effort and uncoordinated contact with passenger rail and rail transit systems, and to close potential gaps in information collection and assessment. This program establishes a formal process for sharing of information and coordinating efforts across the Federal Government, with State and local governments and private stakeholders, during both routine programmatic activities and high threat/incident-driven events. Participating entities include TSA's Mass Transit and Passenger Rail Division, Office of Intelligence, Office of Chief Counsel, and Public Affairs; OGT, and State and local Government Coordination and the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC); and the FTA. This effort has succeeded in knocking down the "stovepiping" and bureaucratic hurdles that have plagued Federal entities handling and disseminating information. The pilot initiative, originally focused on the National Capital Region and supported by APTA and local transit agencies, including Maryland Rail Commuter (MARC), Virginia Railway Express, and WMATA, has transformed into a program—the Mass Transit and Passenger Rail Security Information-Sharing Network—with a nationwide scope.

DHS established the Homeland Security Information Network (HSIN) for stakeholders to use in the various SCCs. The network includes a Public Transit Portal, intended for use as an information-sharing and exchange resource for transit systems throughout the country. An often expressed concern of transit system security officials is the absence of a single source or "one stop shop" for Federal information on transit security. Working through the TCLDR-GCC and SCC and a coordinated arrangement with the Public Transit ISAC, the Public Transportation Portal on HSIN is envisioned to serve that purpose as the gateway to Federal information updates and resources for the mode and information and material developed by the PT-ISAC. Feedback from mass transit and passenger rail systems will help ensure information products meet security needs. A concerted effort to populate the site with useful and timely information is underway.

The Public Transit Portal to HSIN is compatible with DHS principles of sharing sensitive information over secure/encrypted lines. HSIN is a system where individual access is provided to users and is not available for the general public. It can be used in conjunction with the DHS Alerts systems to notify users of the postings of critical information. TSA is working with DHS Office of Grants and Training (OGT) and DOT/FTA to integrate the National Resource Center (NRC) into the Public Transit Portal of HSIN as the Mass Transit Resource Center. The Resource Center will provide a comprehensive database for the transit industry to access

information on a broad spectrum of subjects pertinent to transit security, material not readily available in any consolidated format now.

The Government will coordinate secure communications using a number of tools. FBI's Joint Terrorism Task Forces (JTTFs) located throughout the U.S. provide a DOJ coordinated effort that affords threat support to the majority of the transit systems in the Nation. TSA is coordinating with the JTTFs to access FBI's secure video conference capabilities to enable delivery of national and regional threat briefings to transit systems' security and operations officials. To complement this capability, TSA is working to provide secure telephone equipment on a risk-informed basis to transit systems to further enhance timely communication of classified intelligence information.

3.2.5 Security Training and Awareness Programs

Targeted Security Training Initiative

An area security assessment results indicate a need for more focused effort is security training for transit agency employees. Although an extensive Federal security training program has been implemented since 9/11 – 17 security courses, more than 500 deliveries, more than 78,000 transit employees trained – the assessment results indicated wide variations in the quality of transit agencies' security training programs and an inadequate level of refresher or follow-on training. Well-trained employees are a security force multiplier for security efforts implemented by transit agencies. To elevate the level of training generally, bring greater consistency, and assist agencies in developing and implementing training programs, TSA produced and disseminated a Mass Transit Security Training Program.

The program identifies specific types of training at basic and follow-on levels for particular categories of transit employees. Presented in a readily understandable matrix, it provides effective guidance to transit agency officials in building and implementing training programs for employees working in their systems. To support execution of such training programs, the Transit Security Grant Program offers pre-packaged training options agencies may obtain with grant funding. Agencies taking advantage of this program have their applications expedited for approval to ensure funds are delivered within 90 days of submission. This initiative aims to expand significantly the volume and quality of training for transit employees during 2007.

TSA is partnering with FTA to advance the Mass Transit Security Training Program, providing the mass transit community with expanded opportunities in the following training programs:

1. **Strategic Counter Terrorism for Transit Managers.** This program presents a studied approach to counter-terrorism, enabling transit managers throughout their respective organization to engage in strategic thinking and assessment of terrorist threats and concerns in the development and execution of strategic plans to guard against terrorism.
2. **Terrorist Awareness Recognition and Reaction (TARR).** This program provides training to transportation employees in how to recognize the behaviors associated with terrorist planning activities, including the conducting of surveillance that could be a precursor to attacks against a transportation facility. The program draws upon lessons learned from the experience of international partners in counterterrorism.
3. **CBRNE Incident Awareness for OCC Personnel.** This program provides Operations Control Center (OCC) and other key personnel with practical knowledge and guidelines for effective and appropriate response to explosive, chemical, biological, and radiological threats and incidents.

FTA continues to provide a slate of courses – 17 in all – that afford passenger rail and mass transit agencies a range of options to advance the scope and quality of training of their employees and local security and response partners. The areas covered by these courses include security awareness; emergency response for chemical, biological, radiological, nuclear, and explosives hazards; managing terrorist incidents in rail tunnels, threat management and emergency response for bus and rail hijackings, and the National Incident Management System. The Federal government will continue to devote resources to maintain and expand these course offerings as effective means to build security force multipliers and elevate security posture in passenger rail and mass transit systems.

Connecting Communities

This initiative brings the Federal transportation security partners together with State, local, and tribal government representatives and the local first responder community to discuss security prevention and response efforts and ways to work together effectively to prepare and protect their communities. These forums enhance information and intelligence sharing among partners in transportation security to facilitate prevention and ensure the capacity for rapid and flexible response and recovery to all-hazards events. TSA partners with the FTA on Connecting Communities. This program is addressed among the Public Transportation MOU Annex initiatives.

The MOU annex stipulates that TSA, FTA, and OGT host 12 “Connecting Communities Emergency Response and Preparedness” training workshops to be provided through the National Transit Institute. These two-day workshops enhance security and safety by sharing transit policies, procedures, resources, and effective practices with local first responders that would respond to transit emergencies and discuss emergency management and response, including the role of Federal, State and local emergency management offices to facilitate efficient planning, preparedness and response coordination. In support of this regional engagement effort, area NJTTF representatives will provide presentations on their activities and coordination responsibilities. The most recent sessions of Connecting Communities occurred in Washington D.C. Metropolitan Area, in February 2007 and Houston in March. Additional Connecting Communities forums will occur throughout 2007 consistent with the annex’s goal of 12 sessions per calendar year. Coordination with the Peer Advisory Group will foster achieving this objective.

Safety and Security Roundtables

TSA, FTA, and the DHS OGT co-sponsored the fifth Transit Security and Safety Roundtable in December 2006. The roundtables bring together the security coordinators and safety directors from the Nation’s 50 largest transit agencies and facilitate dialogue between the government, police and safety and security departments, and industry leaders on how best to address current transit safety, security and emergency management challenges. The roundtables provide a forum for mass transit and passenger rail safety and security officials to share effective practices and develop relationships to improve coordination and collaboration. Roundtables occur twice each year, generally in late spring and late fall.

Federal Law Enforcement Training Center-Land Transportation Anti-Terrorism Training Program

Transit employees, such as train conductors and bus drivers, can play a vital role in preventing a terrorist attack. In many cases, they will be in the best position to observe and report the suspicious activities that are the indicators of developing plans and operations. Effective reporting and coordination with law enforcement is essential. The Land Transportation Anti-

Terrorism Training Program (LTATP) provides critical training to transit officials, local law enforcement, and others who have close, regular interaction with passengers. TSA funded eight of these programs through FLETC in FY 2006 and has made a similar commitment for FY 2007. The 1-week LTATP program is designed to enhance protection of land transportation infrastructure, including passenger rail and mass transit operations. The program is offered at eight different regional locations to maximize the training opportunity for transit systems and affiliated law enforcement entities.

Transit Watch

The Transit Watch Program, co-led by FTA and TSA, provides a nationwide safety and security-awareness program designed to encourage the active participation of transit passengers and employees. Via this program, the Federal government, in collaboration with APTA, CTAA, and ATU, has created templates for transit agencies to develop and/or enhance their own public awareness programs. The templates that enable transit agencies to produce awareness materials, such as posters and flyers, with images and logos from their systems inserted, have been distributed nationally in a CD-ROM format. The materials are also accessible through the FTA and TSA public websites and the Public Transit Portal of HSIN.

The "If You See Something, Say Something" campaign is derived from the Transit Watch program. Other materials include Employee Tip-Cards, "Who Owns This Bag" campaign, and a passenger rail pamphlet that includes information on how to dealing with a security threat and monitoring suspicious activities. The program employs a staged approach through basic and more advanced materials to boost public awareness and vigilance, adding a security force multiplier.

National Security Awareness for Railroad Employees, Interactive Computer-Based Training Program

TSA has contracted with the National Transit Institute (NTI) at Rutgers University to develop and distribute 10,000 copies of an interactive computer-based training program for passenger rail, rail transit, and freight rail employees, which will provide employees the practical knowledge and skill sets necessary to identify security threats, observe/report suspicious activities and objects, and take the proper actions(s) to mitigate and/or recover from a threat or incident. The interactive CD-ROMs will be distributed to rail transit and passenger and freight rail systems and access to the Internet/corporate intranet will be offered.

Random High-Visibility Passenger Awareness Program

In a partnership effort with mass transit agencies, this program is designed to disrupt a terrorist's pre-attack activities through a highly visible public-awareness campaign to enhance passenger vigilance and response to possible terrorist activity. The TSA's Mass Transit Division and STSIs joined by the transit agency police or security officials surge during varying dates, times and locations throughout the agency's trains and stations. TSA STSIs display posters and distribute security-awareness information to passengers and system employees. This program does not entail additional expense to transit agencies.

The initial effort took place in 2006 at the Washington Metropolitan Area Transit Authority around the fifth anniversary of September 11 where the WMATA Metro Transit Police Department partnered with TSA STSIs. TSA plans to offer this support throughout 2007 with an objective of conducting joint public awareness campaigns in eight regional areas.

Transit Terrorist Tools and Tactics (T4)

To enhance supervisory and frontline employee training and awareness, the Transit Security Grant Program funded, and the University of Tennessee developed, the Transit Terrorist Tools

and Tactics (T4) course. This intensive 3-day course, provides participants with the knowledge, skills and abilities to detect, deter, prevent, mitigate, and respond to the consequences of a terrorist chemical, biological, radiological, nuclear, and explosive (CBRNE) attack against a transit target. This course was offered to the mass transit community for the first time in the fall of 2006.

3.2.6 National Tunnel Security Initiative

This interagency effort brings together subject matter experts from a range of relevant fields among DHS and DOT organizational elements to identify, assess, and prioritize the risk to mass transit systems in the United States with underwater tunnels and assist transit agencies in planning and implementing protective measures to deter and prevent attacks and blast mitigation and emergency response strategies in the event of a terrorist attack and/or all hazards incident or event. Through regular meetings, this working 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 integrating the overall risk mitigation effort for a cohesive, coordinated, and effective approach. The initiative has:

1. Identified and assessed risk to underwater tunnels
2. Prioritized tunnel risk mitigation based on risk to drive grant funding to most pressing areas
3. Developed strategies for funding future technology research and development aimed at producing novel approaches to this challenging problem.
4. Produced and disseminated recommended protective measures transit agencies may implement to enhance security 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.

3.2.7 Security Technology Deployment

This cooperative initiative between TSA and mass transit and passenger rail stakeholders deploys various security technologies to interested public transportation systems for security supplement and developmental testing. The program introduces the stakeholders to new technology, assists with their screening needs, and conducts surge operations around the United States. A formal process led by DHS Science and Technology (S&T) Directorate and the TSA Chief Technology Office, in full partnership with the public transit community, will identify security technology needs and advance capabilities for the flexible application of mobile and fixed systems to enhance security in public transit environments. Primary activities include planning, coordinating, overseeing, and executing the technology deployment.

A related effort involves risk-based regional deployment of explosive trace detection equipment issued by TSA Mass Transit Security Division. Distribution and training on the equipment will align with the regional collaboration approach to enhance security posture in transit systems. TSA STSIs will receive training on the equipment and provide that training to transit system personnel. The equipment will be deployed randomly and unpredictably, emphasizing mobility, to enhance the deterrent effect.

3.2.8 Technology Research and Development

Public and private partners are working together to evaluate technology needs of Mass Transit and Passenger Rail industry and to develop and coordinate research and development as well as testing and evaluation of commercial off-the-shelf and other existing technologies. Under the Public Transportation Annex of the DHS/DOT MOU discussed earlier, TSA leads the Mass Transit Technology Subgroup consisting of representatives from OGT, FTA, and S&T (as applicable). This subgroup allows for coordination and sharing of ongoing work, discussion of stakeholder needs based on individual agency outreach through their programs, and leveraging of resources to expand the work done in technology by the agencies.

Through Transit Safety and Security Roundtables discussed earlier, stakeholder tours of S&T's Transportation Security Laboratory, interagency informational tours, and other meetings, TSA and its Federal partners exchange information on planned research, development, testing, and evaluation efforts, projects, and needs and challenges with the stakeholders and scientific/technology community. The results are developed into broad requirements submitted to S&T for research and development. Furthermore, TSA participates in the Integrated Project Teams (IPT) held by S&T across a variety of critical infrastructure and potential threats. These IPTs provide a means to submit technology requirements for funding and coordinate requirements with other DHS internal stakeholders (i.e. CBP, Coast Guard) to eliminate duplication of effort and share experience and knowledge. TSA and industry representatives also participate in bi- and multi-lateral international meetings and working groups on technology that focus on sharing of information on a specific technology or broad technology needs and requirements. TSA and its partners are working on a plan to utilize HSIN-Public Transit Portal as the tool to provide government and the industry with a list of available technologies and products relating to the protection of mass transit and passenger rail.

Improved Mass Transit Surveillance and Early Warning System

This research and development project entails developing software analytics to identify human anomalous and suspicious behavior using new and legacy surveillance camera systems. The first phase of testing has and continues to take place in two light rail stations on Metro Transit in Minneapolis, MN. The second phase will take place at Amtrak's 30th Street Station in Philadelphia.

Bus Communications and Control

This program entails research and development of the basic capability to remotely disable a bus and thereby prevent its use as a delivery device for an explosive, chemical, biological, or radiological weapon against a critical infrastructure or crowds of people. The technology will allow a command/operations center to disable a bus that may be compromised, particularly where operators may not be in the position to disable the bus themselves.

On August 1, 2006, TSA, and the Transportation Security Laboratory, conducted a proof of concept test of this technology. TSA partnered with the Orange County Transportation Authority to test the system on board a standard revenue bus. The ability to de-rate the bus while in motion, authenticate the driver for the specific bus, and shutdown the bus when a non-authenticated driver attempted to operate the bus while idling were successfully demonstrated. TSA will test this technology in a field environment in the near future.

Moveable Security Checkpoints

TSA has conducted field testing on a Moveable Security Checkpoint. This mobile equipment, which can fit into two standard size shipping containers, can be rapidly deployed to use in screening and detection at any major system in the country. The equipment has performed effectively in Maryland in the MARC commuter rail system and the Maryland Transit

Administration lightrail system. This is another tool available for deployment at mass transit and passenger rail locations throughout the Nation randomly, in the event of a threat or incident, natural disaster, and during national security special events. TSA has dedicated funding to support deployments of these checkpoints.

National Capital Region Rail Security Corridor Pilot Project

The National Capital Region Rail Security Corridor Pilot Project, conducted through the Preparedness Directorate's Office of Infrastructure Protection, is designed to meet the needs of local law enforcement, first responders, and the Federal Government while supplementing the existing security measures of rail operations in the Washington, DC, area. The pilot project consists of numerous components, including a virtual security fence that detects moving objects, perimeter breaches, left objects, removed objects, and loitering activity along the 7-mile DC Rail Corridor. Data from the fence and the gates will be encrypted and transmitted simultaneously to multiple locations, such as U.S. Capitol Police, U.S. Secret Service, CSX, and other applicable Federal or local agencies. Though primarily focused on freight rail security, the security initiatives undertaken in this project afford benefits to passenger rail systems traveling on the same tracks.

Currently, DHS is evaluating new explosive detection equipment. Through S&T's Rail Security Pilot (RSP), DHS is field testing the effectiveness of explosives detection techniques and imaging technologies in partnership with the Port Authority of New York and New Jersey. These advanced technologies have been tested in the transit environment in the Port Authority Trans-Hudson (PATH) interstate rail system.

Bomb Resistant Trash Cans

The Systems Support Division (SSD) of OGT has conducted operational tests to evaluate manufacturer claims on ballistic resistant trash receptacles and published a report of its findings to help ensure mass transit and passenger rail systems, among others, have the information needed to guide critical procurement decisions. Similarly, SSD has published a Closed Circuit Television (CCTV) Technology Handbook to provide a reference point on current CCTV technologies, capabilities and limitations.

3.2.9 International Initiatives

TSA engages extensively with its foreign counterparts on rail and transit security matters with the aim of sharing and gleaned effective practices for potential integration in the domestic strategic approach. TSA conducts and maintains these efforts in collaboration and coordination with the Department of State, DHS component agencies, and other Federal agencies on projects involving transportation security within international and regional organizations.

Engagement within the Group of 8 (G8) and with the European Union, the Asia Pacific Economic Cooperation, and the Mexican and Canadian governments fosters sharing of effective practices and technologies in mass transit and passenger rail security. The expanding cooperation in this area has culminated in creating an international working group on land transport security outside of any preexisting forum with preliminary focus on passenger rail and mass transit security. The United States will support this collaborative effort by providing information on most effective security practices and the effectiveness of security technologies.

TSA also participates in the Rail and Urban Transport Working Group in support of technology information-sharing across five countries. The membership of this group consists of the United States, United Kingdom, Canada, France, and Israel. In this forum, technology and operational experts come together to share information on technology testing and evaluation projects.

Through the Joint Contact Group, the United States and the United Kingdom engage in a bilateral cooperative effort to develop and promulgate best practices in rail and mass transit security, with the objective of developing security solutions applicable on a wider international basis. This group also explores opportunities to encourage broader private sector involvement in the protection of soft targets, such as through training of mass transit employees.

Another international initiative focuses on vetting suspicious packages detected in transit systems. This joint effort, involving TSA STSIs, Los Angeles law enforcement representatives, and British security officials, will bring training, experience, and lessons learned to the American participants from a British program known as Hidden and Obviously Typical (HOT) of suspicious packages. This program enhances the ability of the trained personnel to identify indicators of security concerns with packages left unattended in transit and rail facilities and vehicles.

TSA will continue a dynamic effort to engage with international counterparts, whether through bilateral arrangements or broader forums and working groups, and advance sharing of lessons learned and best practices to enhance security in passenger rail and mass transit systems.

3.3 Effective Practices, Security Guidelines, Security Standards, and Compliance and Assessments Processes

3.3.1 Security Guidelines

In the immediate aftermath of the terrorist attacks against the U.S. on September 11, 2001, FTA took steps to enhance security posture and practices among transit systems nationwide. FTA established 20 specific action items (Top 20) for transit system security readiness. The action items and supporting references provided an excellent resource to facilitate developing of security plans and programs. FTA used the Top 20 as an assessment tool in assessing the readiness of the Nation's 50 largest transit agencies (through developing of the Red/Yellow/Green stoplight chart), as part of its technical assistance program to the 50 largest transit agencies. FTA also used the Top 20 assessments as a gap analysis tool, to identify areas where transit agencies needed additional guidance. Gap analysis products include a threat level protective measures guidance document discussed below, which was recently updated by FTA and TSA.

As mentioned earlier, the action items recently underwent a comprehensive review and revision in a collaborative effort by FTA and TSA, in coordination with members of the TCLDR-GCC and the Mass Transit SCC. As a result, the newly enhanced Security and Emergency Management Action Items represent a comprehensive and systematic approach to elevate baseline security posture and enhance security program management and implementation. They address the current security risks that confront transit agencies today and priority areas where gaps need to be closed in security and emergency preparedness programs. The 17 Action Items cover a range of areas including security program management and accountability, security and emergency response training, drills and exercises, public awareness, protective measures for Homeland Security Advisory System (HSAS) threat levels, physical security, personnel security, and information-sharing and security. They are accessible on the FTA and TSA public websites and the Public Transit Portal of HSIN.

Through the BASE program, TSA STSIs assess a transit system's security posture on the 17 action items, with particular emphasis on six core Transit Security Fundamentals, discussed in more detail below at section 3.5. The BASE program aims to elevate security generally and expand TSA's awareness and understanding of security posture in the passenger rail and mass transit mode. This information enables more effective targeting of security programs and technical assistance to elevate security. Through this process, TSA also identifies best security practices for sharing with the passenger rail and mass transit community, further enhancing security posture. The thorough review of security programs and procedures affords the systems assessed the opportunity to review the state of their security program and identify strengths and weaknesses. This information can guide the effective application of available security resources, focus collaborative efforts with TSA, and facilitate the preparation of funding requests through security grant programs.

Another jointly developed product by TSA and FTA, also coordinated with the Mass Transit SCC, is the recommended protective measures for the threat levels under the HSAS. This product is an update of the Transit Threat Level Response Recommendation product FTA developed to provide guidance to the U.S. transit industry in responding to the threat level designations set by the then Office of Homeland Security. The current recommended protective measures reflect the advantages of improved threat and intelligence information, security assessments conducted by FTA and TSA, operational experience since the 9/11 attacks that prompted the original version, and collective subject matter expertise and experience of Federal

partners and the transit community. This product has been developed as a technical resource to transit agency executive management and senior staff assigned to develop security and emergency response plans and to implement protective measures for response to the HSAS threat conditions and emergencies that might affect a transit agency. The updated protective measures may be accessed at the Public Transit Portal to HSIN.

FTA and TSA and other relevant entities will work together, within the Risk Assessment and Security Review Working Group of the Public Transportation Annex to the DHS/DOT MOU and in the context of the TCLDR-GCC and the Mass Transit SCC, to further apply the results of security assessments to develop guidance materials in various areas to foster enhanced security programs and practices. Examples include continued development of the Transit Watch program and the preparation of guidance documents for conducting of transportation workers background checks and handling of sensitive security information.

A key component of this effort is the developing Next Generation Technical Assistance Program. Elements of this program will include (1) developing a safety, security and emergency management baseline master plan and planning process, and (2) continuing to produce industry useful guidance documents through the gap analysis process.

3.3.2 Security Standards Development

The Federal Government is engaging with the APTA Security Standards Policy and Planning Committee to develop security standards. In transit safety, APTA has been actively involved in transit industry standards development for over nine years and is recognized by the federal government and other standards organizations as a “Standards Development Organization.” The security standards development effort brings together security professionals from the public transportation industry, business partner representatives, and the Federal Government in a collaborative effort to develop consensus-based standards to enhance security in transit systems. Federal participants consist of the subject-matter experts from DHS OGT, TSA (Mass Transit and Passenger Rail Division and STSI Program), FTA, and FRA. Public transportation stakeholder participants consist of members of the APTA Security Standards Policy and Planning Committee, officials from mass transit and passenger rail systems and industry businesses and research organizations. Working groups are established to focus on specific security areas and concerns, including mass transit and passenger rail systems, facilities and operations.

As an example, the Transit Security Infrastructure Working Group is working to develop industry standards for transit-related infrastructure. Transit infrastructure is defined as passenger, maintenance and operations facilities, and their related assets; rights-of-way, including tunnels, elevated structures, and bridges; fixed assets, such as track, signals, traction power substations, and interlockings. The working group will initially focus on the types, placement, and testing of trash receptacles, lighting and fencing and CCTV. Working groups have also been formed and are beginning efforts on developing standards for the next two areas: risk assessments and emergency drills and exercises.

Draft standards are developed in a format that is consistent with American National Standards Institute (ANSI) requirements and are posted for comment and then approved by consensus. Federal participation in the consensus-based efforts is effected through the GCC/SCC framework and CIPAC process. The approved standards are then put forth as "recommended practices" and supported by the American Public Transportation Association for voluntary adoption by the transit industry.

3.3.3 Security Directives

TSA issued two security directives applicable to passenger rail and mass transit systems in the aftermath of the attacks on commuter trains in Madrid in March 2004 pursuant to its authority under 49 U.S.C. § 114(l). The directives, designated SD RAILPAX-04-01 and SD RAILPAX-04-02, mandate specific measures intended to enhance the security of the U.S. passenger rail and mass transit modes. The security directives underwent coordination and collaboration with other Federal agencies, as well as consultation with the stakeholder community, and were approved by the Secretary of Homeland Security and the Transportation Security Oversight Board.

The measures the directives require support DHS's overarching goals of prevent, protect, respond, and restore. They have the force of regulations and remain valid and effective until revised or superseded by TSA's subsequent action.

TSA and the Transit Policing and Security Peer Advisory Group, under the auspices of the Mass Transit SCC, have developed a 1-year business plan for mass transit and passenger rail security. (See section 4) A component of the plan for 2006–2007 is a review of the specific measures under the security directives to ensure the requirements remain viable in enhancing security in the current security and operational environment. On the business plan concept, we anticipate reviewing progress annually and setting new objectives based on the progress achieved and prevailing security circumstances. The plans will be reviewed through the GCC/ SCC structure.

3.3.4 Notice of Proposed Rulemaking

TSA issued a Notice of Proposed Rulemaking (NPRM) on December 21, 2006 that, although primarily focused on security in transporting toxic inhalation hazard (TIH) material by freight rail carriers, imposes some requirements on certain passenger railroad carriers, rail transit systems, and hosts of passenger rail service. The requirements include designation of a primary and at least one alternate Rail Security Coordinator to serve as the point of contact with TSA on security matters and communications and to provide oversight to the railroad carrier or rail transit system's compliance with security requirements and implementation of security initiatives. Additionally, in recognition of the vital importance of information indicating terrorist planning and preparation, the rule further requires all passenger rail carriers and rail transit systems to report potential threats or significant security concerns to TSA's Transportation Security Operations Center (TSOC).¹⁸ The draft rule also details TSA's authority concerning inspection of the facilities and operations of covered passenger rail and rail transit systems and hosts of passenger rail service.

This NPRM provided ample time for comments by stakeholders and the public at large. A public meeting was held on February 2 to provide further opportunity for comments. TSA is reviewing the comments and making the appropriate changes, if any, to the proposed rule.

3.4 Grant Programs

Through the Transit Security Grant Program (TSGP), DHS has allocated \$547 million to date to 60 of the Nation's mass transit and passenger rail systems in 25 states and the District of Columbia. The TSGP employs risk-based prioritization consistent with TSSP. This approach applies TSGP resources to generate the highest return on investment and, as a result, strengthen the security of the Nation's transit systems in the most effective and efficient manner. The rail transit systems have been divided into two tiers based on risk. Particular emphasis is placed on the passenger volume of the system and the underwater and underground infrastructure of the rail transit systems. Tier I systems apply for a portion of a regional

¹⁸ These requirements are presently included in Security Directives, SD RAILPAX 04-01 and SD RAILPAX 04-02

allocation, either as individual agencies or as part of regional projects that mitigate the vulnerability of high-risk, high-consequence assets. Grants for systems in Tier II are competitively awarded based on the ability to reduce risk, cost effectiveness, and the ability to complete the proposed project with the funds awarded.

The bus transit systems have been divided into two tiers based on risk as well. Particular emphasis is placed on ridership, passenger miles, and the number of buses in the system. Tier I systems apply against awarded allocations. Grants for bus systems in Tier II are competitively awarded based on the same factors (described more fully in Part II) of ability to reduce risk, cost effectiveness, and likelihood of project completion using the funds awarded. Ferry systems apply against regional allocations, similar to the Tier 1 areas in the rail transit and bus grants.

The application of risk-based priorities is being institutionalized by developing a regulation governing the Transit Security Grant Program. Mandated under the SAFETEA-LU,¹⁹ DHS and DOT will jointly issue the rule. The draft rule places particular emphasis on ensuring transit systems enhance their capabilities in implementing six core fundamentals that provide the essential foundation for effective security programs. The Transit Security Fundamentals are:

1. **Protection of high risk underwater/underground assets and systems.** Because of the consequences of IED attacks in an enclosed environment where there may also be large concentrations of riders, protecting riders and the integrity of the transit system against such attacks is essential. Transit agencies should focus countermeasures on programs that can prevent an attack or mitigate the consequences of an incident. Active coordination and regular testing of emergency evacuation plans can also greatly reduce loss of life.
2. **Protection of other high risk assets that have been identified through system-wide risk assessments.** It is imperative that transit agencies focus countermeasure resources on their highest risk, highest consequence assets. 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. For example, using smart CCTV systems in remote locations can help free up security patrols to focus on more high-risk areas.
3. **Use of visible, unpredictable deterrence.** Visible and unpredictable security patrols have proven to be very successful for instilling confidence and calm in the riding public and, most importantly, in deterring attacks. These kinds of patrols, especially those employing explosives detection canine teams or mobile screening or detection equipment, represent effective means to prevent and deter IED attacks. Security patrols should be properly trained in counter-terrorism surveillance techniques. An understanding of terrorist behavior patterns helps security patrols more effectively intervene during terrorist surveillance activities or the actual placing of an IED.
4. **Targeted counter-terrorism training for key front-line staff.** Appropriate training enhances detection and prevention capabilities and ensures a rapid, prepared response in the first critical minutes after an attack—steps that can significantly reduce the consequences of the attack. 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.

¹⁹ Safe, Affordable, Flexible, Efficient Transportation Equity Act – A Legacy for Users, Public Law 109-59, August 10, 2005

5. **Emergency preparedness drills and exercises.** Experience has taught transit agencies that well-designed and regularly practiced drills and exercises are fundamental to rapid and effective response and recovery. Transit agencies should develop meaningful exercises, including covert testing, that test their response effectiveness and how well they coordinate with first responders. In addition to large regional drills, transit systems should also conduct regular, transit-focused drills. Drills should test response and recovery to both natural disasters, as well as, terrorist attacks.
6. **Public awareness and preparedness campaigns.** Successful security programs in all industries understand the value and power of the public's "eyes and ears." Awareness programs should be well-designed and employ innovative ways to engage the riding public to become part of their "transit security system." Advertisement campaigns, using media and celebrity support have proven to be very successful. Including the riding public in preparedness and evacuation drills has also been shown to be effective in raising public awareness. A transit agency's awareness campaign should also extend to its employees. Appropriate counter-terrorism training, coupled with a strong security awareness campaign, will yield significantly heightened security awareness in transit systems.

3.5 Way Forward

The Federal Government recognizes the value of consensus-based decision making at every level of engagement with the public transportation industry to develop strategies and programs for enhancing security posture and practices throughout the mode while complying with applicable legal requirements. A major step in the process is being reached through the TCLDR-GCC and the Mass Transit SCC and through the CIPAC process at the national level. This process facilitates coordination on developing security strategies, programs, and initiatives and allows for a more effective execution of the Executive Order on surface transportation security, the successful implementation of which would not be possible without collective engagement and consensus-based decision-making process.

The current organizational and funding construct for TSA's Mass Transit Security Division imposes some significant challenges, namely in available funding and staff. TSA is committed to taking steps to ensure an appropriate alignment of resources with responsibilities. State and local governments grapple with resource constraints as well. The mass transit and passenger rail industry continually tries to balance operational demands and costs and maintain an effective level of security. We must ensure, through a risk-based approach, to maximize the security effectiveness of the resources available. Program dollars should support security enhancements and security grant dollars should be utilized to mitigate identified vulnerabilities outlined in security plans benefiting preparedness for all manners of hazards, including natural disasters.

TSA is leading the formation of regional public transportation GCCs and encouraging public transportation stakeholders in metropolitan areas throughout the United States to form regional SCCs. These councils will foster development and communication of coordinated policies and positions on matters in transportation security and operational efficiency. Members of the respective councils would engage in collaborative efforts to develop and implement security strategies, plans, and programs under the CIPAC.

The regional approach fosters security collaboration and coordination. Potential stakeholder participants could encompass all public transportation modes servicing a regional area.

Participants in a regional public transportation GCC may include regional representatives of:

- TSA (Federal Security Director or designee, STSIs, FAMs)
- DHS officials serving in the area, if available (such as a DHS Protective Security Inspector or representatives of CBP and/or Immigration and Customs Enforcement (ICE))
- Regional DOT personnel (such as FRA field inspectors and FTA regional office representatives)
- The U.S. Coast Guard detachment in the area, if applicable
- SSOA representative²⁰
- State Homeland Security Advisor, county, or local homeland security officials
- FBI's NJTTFs and other Federal, State, tribal, and local law enforcement entities with jurisdiction in the area
- Other governmental first responders, such as fire departments in the area

The developing model framework encourages such initiatives and aligns their development and implementation with the public-private partnership model envisioned under HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection*, and effected by the NIPP and the

²⁰ Designated per 49 CFR Part 659

TSSP. This approach calls for the establishing regional transportation government coordinating councils in areas where TSA security officials are assigned. The Federal Security Director or his designee, such as an Area Director for the Surface Transportation Security Inspection Program, engages area Federal, State, and local government officials responsible for transportation security.

- ❑ Bringing governmental partners together in this fashion creates a regional security network to yield greatly expanded domain awareness, improved sharing of timely national and regional security information, mutual understanding of capabilities and needs, and integrated security approaches that maximize the impact of available resources.
- ❑ Regional councils can take strategic and tactical outlooks, fostering the development and implementation of security activities that harness the full spectrum of assets in the particular area in innovative, random, and unpredictable ways.
- ❑ The networked approach to regional public transportation security advances the overall mission objectives to detect, deter, and prevent terrorist attacks and build a coordinated and effective capacity for response and recovery should an attack occur.

These regional government councils should encourage transportation stakeholders to form regional sector coordinating councils. Neither an individual government agency nor a regional GCC may direct forming a regional SCC. However, governmental entities may encourage such organizing to facilitate collaborative efforts on the full spectrum of security issues.

In regional areas encompassing ports, the existing Area Maritime Security Committee structure would include key governmental partners and regional transportation stakeholders. This existing structure should be leveraged to facilitate the broader transportation security coordination envisioned under the proposed regional GCC/SCC framework.

3.6 Metrics

General

To evaluate the collective impact of the mass transit and passenger rail public-private partnership efforts to mitigate risks to and increase resilience of systems and assets, measures of effectiveness must be developed and monitored. Metrics supply the data to affirm that specific goals are being met or to show what corrective actions may be required. To be effective, the NIPP measurement program requires the cooperation of all modal GCCs and SCCs to provide accurate responses to the metrics being used to measure sector risk posture, and the effectiveness of the Sector-Specific Plan (SSP).

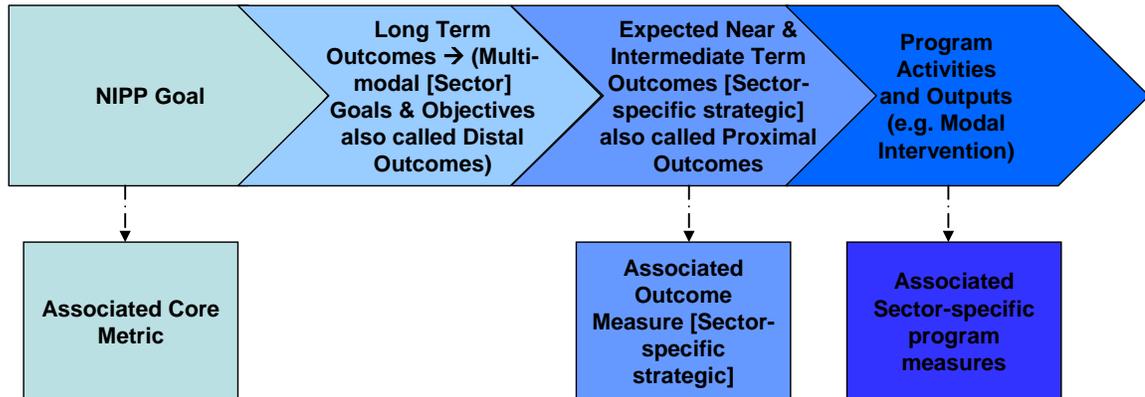
Measurement Joint Working Group

A Measurement Joint Working Group will be formed under the Transportation Sector GCC and Transportation Sector Coordinating Council (TSCC) and will be comprised of one member from each modal GCC and SCC or their designee and invited measurement professionals. TSA's lead measurement organization will chair the group to operationalize measures, establish data sources, data collection and verification procedures, set measurement policy for the TSSP, and approve supporting procedures. The Measurement Joint Working Group will communicate regularly with Transportation Sector GCC/SCC members to ensure that its progress and plans are fully transparent and are agreed upon by the members. In addition, work products of the Measurement Joint Working Group will be submitted, when appropriate, to the overarching Transportation Sector GCC/SCC for approval.

Measures

The Outcome Monitoring Methodology as shown in figure 3-5 demonstrates working down from the national and multi-modal (sector) goals to determine outcomes and their respective measures.

Figure 3-5: Outcome Model



As discussed in section 6 of the TSSP Base Plan, the Transportation Sector’s metrics have been segmented into two categories comprised of three types of measures. The three types are:

1. Core. Core NIPP metrics are common across all sectors and focus on measuring risk reduction progress in the sector. These measures are often descriptive statistics (counts). Following is an example of mass transit and passenger rail NIPP core metrics:

“Number of mass transit assets/systems/networks that have performed a vulnerability assessment”

2. Sector-specific strategic. These metrics are used to gauge the overall effectiveness of mass transit and passenger rail and other modes toward meeting TSSP goals and objectives. Ordinarily, these are outcome measures capable of quantifying the degree to which the SSP is “affecting” sector security. In the early stages of the program, substitute output measures may need to serve as proxies for the long-term outcome measures. In this instance, output data is likely to be collected from the mode and combined at the sector level (or reported independently at the mode level).
3. Sector-specific program. These measures are aligned to the strategic risk objectives (i.e. priorities, strategies, etc.) for the Transportation Sector. “Strategic Risk Objectives” for the sector will be developed consistent with the discussion in Chapter 3 of the TSSP Base Plan. Strategic risk objectives are developed with program measures and should be aligned to the overall TSSP goals and objectives. Standard performance measurement techniques for mass transit and passenger rail programs will be supplemented with measures to demonstrate how the program is meeting associated TSSP strategic risk objectives.

4 Program Management

The initiatives, programs, and processes devised by and through the public-private partnership model and enumerated in this annex for the security of mass transit and passenger rail seek to prevent acts of terrorism against the systems through creating a secure, resilient, and efficient public transportation network employing a flexible, layered, and unpredictable approach based on risk management principles articulated in the NIPP. Ensuring security in mass transit and passenger rail systems is a dynamic process requiring coordinated and collaborative efforts among Federal Government entities, State and local governments, and mass transit and passenger rail stakeholders.

Using the GCC/SCC framework and through the CIPAC process, this Implementation Plan for Mass Transit and Passenger Rail will be reviewed and updated periodically. The TCLDR-GCC will facilitate this process by holding periodic meetings and by working in collaboration with the Mass Transit SCC to review and update the plan.

In this context, TSA has engaged with its governmental partners and private sector representatives to finalize a Business/Action Plan for 2007. The plan calls for establishing of a Transit Policing and Security Peer Advisory Group consisting of transit police chiefs and security directors representative of the constituency. This group has been established within the Modal GCC/SCC under the framework provided by CIPAC. Its membership consists of 13 transit security chiefs and directors from systems across the country of varying sizes. The Peer Advisory Group meets at least quarterly, either in person or via teleconferencing.

The business plan further stipulates the following:

Communications/Information Sharing

- ❑ Under the auspices of the interagency Mass Transit and Passenger Rail Security Information Sharing Network consisting of security officials and staff experts (e.g., intelligence, technology, legal) from TSA, FTA, and appropriate DHS offices, and within the context of CIPAC, the TSA Mass Transit and Passenger Rail General Manager will facilitate monthly information and issues teleconferences with transit security industry partners.
- ❑ The ISACs' functions and processes will be integrated with the intelligence analysis and products from DHS HITRAC and TSA's Office of Intelligence and the interagency coordination and collaboration afforded by the Mass Transit Security Information Sharing Network, as need to know allows. This integrated effort will support the broader information-sharing efforts currently dedicated to expanding use of the Homeland Security Information Network's Public Transit Portal and the developing National Resource Center as a key component of the Portal.
- ❑ TSA and peer advisory group will establish a web-based database of agency contacts and effective security practices.

Security Guidelines and Standards Development

- ❑ TSA and FTA, in coordination with the Mass Transit SCC, will regularly review and, as necessary, update the Security and Emergency Preparedness Action Items and the HSAS Recommended Protective Measures. This dynamic approach will ensure these products continue to address current risks and reflect the most effective baseline security measures and practices. As part of this effort, TSA and FTA will conduct an

evaluation of the results of security assessments to develop specific recommendations on effective security measures and practices.

- ❑ TSA will work with the TCLDR-GCC, the Mass Transit SCC, and the Transit Policing and Security Peer Advisory Group, within the context of CIPAC, to continue to advance the development of security standards, potentially integrating a tier-based program. Developing this program may model the National Law Enforcement Accreditation Program. The security standards program will include a self-assessment module.
- ❑ TSA will continue to offer security assessments by Surface Transportation Security Inspectors under the BASE program to review passenger rail and mass transit systems' security posture on the 17 Security Action and Emergency Preparedness Action Items. The assessment checklist may also be provided to systems for the conduct of self-assessments in advance of an STSI-led review and to guide internal security audits. Additionally, working through the Transit Policing and Security Peer Advisory Group, TSA will coordinate conduct of self-assessments by the Top 50 transit agencies on the six Transit Security Fundamentals.
- ❑ Where self-assessments are conducted, TSA STSIs will follow-up to verify the results and engage in an informed discussion on the systems' security posture based on NIPP's risk assessment principles.
- ❑ TSA will consult with the Transit Policing and Security Peer Advisory Group under the CIPAC process to establish model security practices and guidelines similar to the APTA/FTA Security Guidelines Manual.

Training

- ❑ TSA will work with regional public and private partners to develop and sponsor regional emergency preparedness drills. TSA will determine and inform the regional partners of funding availability for drills.
- ❑ TSA will continue its involvement in international forums dedicated to advancing mass transit and passenger rail security. In addition, TSA will continue efforts to develop international exchange and study tours to expand the application of security lessons learned, best practices, training techniques, and other useful information between transit security practitioners in the US and other countries. This effort aims to lay the foundation for beneficial exchanges of security professionals serving in high-risk, high-consequence transit agencies.
- ❑ TSA, in collaboration with FTA and the Mass Transit SCC, will establish a peer-to-peer program to provide subject matter experts to local transit security professionals.
- ❑ TSA will sponsor seminars focused on tactical response teams and training and determine and inform the regional public and private partners of funding availability for this effort.
- ❑ TSA will work with FTA to evaluate the state of transit security training generally, identify gaps, and develop and implement programs to close those gaps. Implemented in coordination with the Mass Transit SCC and the Transit Security and Policing Peer Advisory Group, this effort aims to advance development of a broad variety of training courses to enhance the capabilities of transit system employees, law enforcement professionals, and first responders.

Security Technologies and Research and Development

- ❑ Through the Mass Transit Security Technology Working Group, formed under the auspices of the Public Transportation Annex to the DHS/DOT MOU, TSA, FTA, OGT will work with the Mass Transit SCC and the Transit Policing and Security Peer Advisory Group, employing the CIPAC process as necessary, to develop a priority research and development action plan.
- ❑ TSA, FTA, and OGT will establish a web-based information resource on operating standards and specifications for security technologies. This effort includes establishing priorities to ensure the availability of information on existing technologies in the most expeditious manner, leveraging testing work already completed and databases, such as OGT's SAVER network, already developed.
- ❑ TSA and the Transit Policing and Security Peer Advisory Group will establish a database of technologies deployed by various transit systems. This information will facilitate networking and sharing of lessons learned among mass transit and passenger rail systems to enhance the employment of security technologies.
- ❑ TSA, working with DHS S&T, will establish and conduct pilot testing to advance development of flexible security solutions and enhance deterrence through visible, random, and unpredictable employment of security technologies.

5 Mass Transit and Passenger Rail Security Gaps

The following is a description of security gaps that are currently being addressed in each of the programs and processes listed in Section 3.2 of this annex.

This information is in part derived from the data generated using results of Baseline Assessment and Security Enhancement reviews completed to date by the Surface Transportation Security Inspection Program at TSA and reflects the current implementation status of the Transit Security Fundamentals and the FTA/TSA Security and Emergency Management Action Items.

1. Information Sharing

There are two security gaps in information sharing:

1. Not all of the top 100 transit agencies have enrolled in HISN.
2. The ability to disseminate such material to properly cleared transit agency officials in a timely manner.

Although the Public Transit portal to the Homeland Security Information Network (PT-HSIN) is fully operational, expansion of the range of invitees will proceed as vetting of the initial enrollees is completed. Although secure, the system does not allow for transmission of classified information. For classified communications work continues to expand the number of systems with cleared officials, to deploy secure communications equipment, and to leverage existing classified communications networks, such as the FBI's secure videoconferencing system aligned with the Joint Terrorism Task Forces.

2. Employee Security Training

The BASE program findings indicate that while many transit agencies provide initial anti-terrorism training to their employees, adequate refresher training is not being provided. Furthermore, the findings indicate that security orientation and awareness training as well as emergency response training is not adequately reinforced. Gaps in training in

these and other areas, such as agency developed incident response protocols, incident command systems, National Incident Management System (NIMS), and Improvised Explosive Device/Weapons of Mass Destruction, are being addressed through the development of a Mass Transit Security Training Program and the Transit Security Grant Program (TSGP).

TSA has developed and disseminated the Mass Transit Security Training Program to guide transit agencies' implementation of effective training. Basic and follow-on training areas are cited, with the categories of employees in a transit agency that should receive the particular types of training. Available Federal course offerings are cited as well. To facilitate prompt action to upgrade training, a pre-prepared training application has been developed under the TSGP. Transit agencies request particular types of training for the various categories of employees. Grant awards cover the cost of training and of overtime or related expenses to backfill employees in classes. TSA is committed to expedited processing to get funds to transit agencies.

3. Security Awareness Campaigns

There is a lack of well-designed public awareness campaigns that employ innovative ways to engage and inform transit riders and employees. Both the public and employees play an integral role in the success of mass transit and passenger rail security programs. Advertisement campaigns, using various forms of media and local officials or celebrity support, that can be easily tailored to the needs of specific agency and locality should be developed and widely disseminated. Resources such as radio and television outlets should broadcast such messages as part of their public service.

The riding public should be included in preparedness and evacuation drills. Transit agencies should be encouraged and assisted to conduct local public outreach and identify individuals willing to participate in such drills and exercises. A transit agency's awareness campaign should also extend to its employees. Appropriate counter-terrorism training, coupled with a strong security awareness campaign, will result in heightened security awareness in transit systems. Additional efforts to conduct outreach and engage transit agencies will further enhance awareness campaigns.

4. Research and Development and Technology Deployment

There is a research and development gap to close or mitigate known security vulnerabilities. For example, we have identified the need for conducting blast modeling for underwater tunnels and DHS/S&T is in the process of engaging National Laboratories to conduct these tests.

In this area, there is also a need for expedited means to identify and test explosive detection devices that are responsive to the high throughput in public transportation environments such as crowded stations. Mass transit and passenger rail systems also lack integrated systems that combine CCTV technology with infra-red capabilities, and alert systems which identify anomalous behavior or objects.

Finally, TSA needs to expand the range of technology tools available for deployment in joint exercises with transit agencies under the Visible Intermodal Prevention and Response (VIPR) program. Expanded regional availability of explosives trace detection equipment will augment the effectiveness of the joint security exercises.

5. Mitigation Strategies for Underwater/underground Tunnels

We have identified a gap in underwater tunnel security because some tunnels are structurally more vulnerable than others depending on the material used to build and maintain them and their position in the river and proximity to the riverbed. TSA led formation of an interagency Tunnel Risk Mitigation Working Group, bringing together subject matter experts from multiple Federal agencies and offices. Broader integration of transit agencies with underwater infrastructure remains necessary. Although this group has systematically assessed security gaps in underwater/underground tunnels, more work remains. Federal and industry partners have taken steps to mitigate these vulnerabilities. Currently, however, we remain in the early stages of developing and implementing a comprehensive risk mitigation effort.

6. Drills and Exercises

.Broader effort is necessary to engage regional security partners – area law enforcement agencies and fire and emergency response units – to ensure thorough familiarity with the operating environment, interoperable communications capabilities, and development of coordinated command and control. Results of the BASE reviews indicate transit agencies are generally doing well in conducting drills and exercises. More effort is needed in leveraging national exercises capabilities developed at DHS and adapting for application to transit agencies in regional exercises. Facilitating this expanded effort through targeted grant funding for cross-functional, interagency regional exercises is a strategic priority for TSA.