



governmentattic.org

"Rummaging in the government's attic"

Description of document: Each substantial Transportation Security Administration (TSA) report to Congress or a congressional committee, 2008-2010

Request date: 15-February-2010

Released date: 13-January-2015

Posted date: 09-February-2015

Source of document: Transportation Security Administration
Office of Civil Rights & Liberties, Ombudsman, and Travel
Engagement (CRL/OTE)
ATTN: Freedom of Information Act Office
601 South 12th Street
Arlington, VA 20598-6033
Fax: 571-227-1406
E-mail: FOIA@tsa.dhs.gov

The governmentattic.org web site ("the site") is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.



**Transportation
Security
Administration**

3600.1

FOIA Case Number: 2010-TSFO-00595

Old FOIA Case Number: TSA10-0333

January 13, 2015

This letter is in response to your Freedom of Information Act (FOIA) request to the Transportation Security Administration (TSA) dated February 15, 2010, in which you requested a copy of each substantial report from TSA to Congress or a congressional committee between January 1, 2008, and the date of your request that is not published on the TSA website.

Your request has been processed under the FOIA, 5 U.S.C. § 552.

A reasonable search within the TSA was conducted and 837 pages responsive to your request were located. Portions of some of the pages are being withheld pursuant to FOIA Exemption (b)(3). A more complete explanation of this exemption is provided below.

Exemption (b)(3)

This information reveals Sensitive Security Information (SSI) and is exempt from disclosure under Exemption (b)(3), which permits the withholding of records specifically exempted from disclosure by another Federal statute. Title 49 U.S.C. Section 114(r) exempts from disclosure SSI that "would be detrimental to the security of transportation" if disclosed. The TSA regulations implementing Section 114(r) are found in 49 CFR Part 1520.

Fees

The fees incurred to process your request do not exceed the minimum threshold necessary for charge and, therefore, there are no fees associated with processing this request.

Administrative Appeal

In the event that you may wish to appeal this determination, an administrative appeal may be made in writing to Kimberly Walton, Assistant Administrator, Office of Civil Rights & Liberties,

Ombudsman and Traveler Engagement, Transportation Security Administration, 601 South 12th Street, East Building, E7-121S, Arlington, VA 20598-6033. Your appeal **must be submitted within 60 days** from the date of this determination. It should contain your FOIA request number and state, to the extent possible, the reasons why you believe the initial determination should be reversed. In addition, the envelope in which the appeal is mailed in should be prominently marked "FOIA Appeal." Please note that the Assistant Administrator's determination of the appeal will be administratively final.

In an effort to maintain a more robust/efficient process to streamline reporting requirements, the TSA, through the Department of Homeland Security, converted to a new FOIA tracking system in October 2013. This modification has resulted in the inability to continue tracking requests with the tracking number assigned by the old system, and changed our naming convention. We are referencing both old and new tracking numbers in our response. I apologize for any confusion this may cause and appreciate your understanding.

If you have any questions pertaining to your request, please feel free to contact the FOIA Branch at 1-866-364-2872 or locally at 571-227-2300.

Sincerely,

A handwritten signature in blue ink, appearing to read "Teri Miller" or "Amanda Deplitch".

Teri M. Miller or Amanda Deplitch
Acting FOIA Branch Officers

Enclosure

Transportation Security Information Sharing Plan



Implementing Recommendations of the
9/11 Commission Act of 2007, Pub. L. 110-53, dated August 3, 2007
Section 1203

July 2008

Department of Homeland Security
Transportation Security Administration

52 **Table of Contents**

53			
54	Executive Summary		i
55	1. Introduction		1
56	1.1. Purpose		1
57	1.2. Scope		1
58	1.3. Relevant Legislation & Guidance		1
59	1.4. Plan Coordination Process		2
60	2. Current State of Transportation Sharing		2
61	2.1. Network Model		2
62	2.2. Current Information Sharing		3
63	3. Transportation Security Information Sharing		4
64	3.1. Defining our Goals		5
65	3.2. Guiding Principles		5
66	3.3. Information Sharing Environment Framework		6
67	3.3.1. Privacy		6
68	3.3.2. Security		6
69	3.4. Adoption of the Information Sharing Environment		7
70	3.4.1. Sharing Information at the Federal Level		7
71	3.4.2. Sharing Information with State, Local and Tribal Governments		8
72	3.4.3. Sharing Information with the Private Sector		9
73	3.4.4. Sharing Information with the Foreign Partners		10
74	3.5. Specific Implementation Actions		11
75	4. Resources and Schedule		12
76	4.1. Resource Estimates		12
77	4.2. Implementation Schedule		12
78	Appendix (A)		A-1
79	Appendix (B)		B-1
80	Appendix (C)		C-1

Executive Summary

Strengthening our Nation's ability to share terrorism information constitutes a cornerstone of our national strategy to protect the transportation system. The Transportation Security Information Sharing Plan (TSISP) establishes the steps necessary to build the foundation for sharing transportation security information between all entities that have a stake in protecting the Nation's transportation system - Federal, State, local, and tribal government agencies, the private sector and foreign partners. This plan reflects the Department of Homeland Security's (DHS) shift from a strictly hierarchical to a networked model, allowing distribution and access to information both vertically and horizontally, as well as the ability to enable decentralized decision making and actions. It builds on the progress of the past five years with the goal of improving the way that all stakeholder parties share information and fight terrorism.

This plan meets the requirements of Section 1203 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*, which requires that the Secretary of Homeland Security establish the TSISP in coordination with the Program Manager of the Information Sharing Environment (PM-ISE), the Secretary of Transportation, and public and private stakeholders. The plan considers the full range of information sharing among the public and private sectors and leverages the progress already made to get the right information to the right people at the right time. The TSISP is closely aligned and consistent with the National Strategy for Information Sharing, the Information Sharing Environment Implementation Plan (ISE-IP), the National Infrastructure Protection Plan and the corresponding Transportation Systems Sector Specific Plan.

The goals established in this plan are derived from ISE-IP and focus on effectively sharing transportation security information in order to maintain the security of the Nation's transportation network. The goals for the sharing of transportation information are:

Transportation Security Information Sharing Plan Goals

1. **Multi-Directional Sharing:** Establish a framework enabling secure, multidirectional transportation security information sharing between government and industry
2. **Effective and Efficient Processes:** Establish clear governance, roles, responsibilities, and communication protocols between transportation security stakeholders to promote more rapid and effective exchange of information, analysis, and coordination
3. **Trusted Partnership:** Establish trusted partnerships among all levels of the transportation security network
4. **Right Information-Right People-Right Time:** Improve the timely and secure exchange of transportation security information supported by education, training, awareness programs, and enabling technologies
5. **Protect Privacy and Civil Liberties:** Ensure privacy and civil liberties are protected within the transportation security network

Information sharing is a multi-directional activity that occurs informally through relationships and more formally through communication policies, regulations, procedures, guidance and tools. Intelligence and information sharing are at the core of the overall transportation security strategy. Currently the primary environments for sharing transportation security information and coordinating intelligence activities at DHS are categorized into four general areas:

1. **Information Sharing Environment.** Aligned first with the DHS-ISE then to the PM-ISE, the Transportation Security Administration (TSA) is designated the lead to establish the Transportation ISE. DHS has begun by building the necessary foundation to provide these mission capabilities internally so it will be better equipped to support these capabilities across the transportation network in the future. This plan lays out steps to evolve and expand the ISE framework.
2. **Office of Intelligence.** Within DHS, TSA has maintained the lead on transportation-related intelligence and analysis. TSA's intelligence mission is to provide timely and accurate intelligence and information related to threats to transportation to TSA and DHS leadership, field entities, and other Federal, State, local, and tribal authorities, and foreign partners. It functions as the conduit between the public and private transportation security stakeholders and the Intelligence Community via DHS's Office of Intelligence and Analysis (DHS I&A).
3. **Sector Partnership Model.** DHS, vis-à-vis TSA and the U.S. Coast Guard in collaboration with DOT and other security partners will continue to leverage and improve partnerships within the Transportation Systems Sector, specifically enhancing the role of the Transportation Systems Sector Government Coordinating Council and Sector Coordinating Council structures as a primary environment in which to collaborate, develop, coordinate and share policy, strategy, plans, challenges, gaps and potential requirements.
4. **Transportation Security Operations Center.** It is the primary coordination point for multiple agencies dealing with transportation security on a daily basis. It serves as a single point of contact for security-related incidents or crises in all modes of transportation.

This implementation plan focuses on the core capabilities needed to maximize information sharing across all communities of interest. As the security framework for transportation continues to grow, TSA and its Federal partners are moving to apply many of these capabilities to reduce risk across all modes of transportation. The mission capabilities and the processes described in this plan will enhance these current functions and will be leveraged across the transportation system. In addition, as our information sharing efforts mature, policy and technology will lead to the introduction of additional information sources not currently included or available with these communities.

The plan calls for a multiple-phase implementation of the TSISP occurring over several fiscal years, with initial activities focused on the expansion of mission capabilities within DHS and the foundational components necessary to expand mission services to other Federal agencies. It calls for subsequent phases to deploy mission capabilities, based on stakeholder prioritization, to other Federal, State, local and tribal, private sector stakeholders, and foreign partners in addition to the continuation of advancements in DHS workspaces.

1. Introduction

1.1. Purpose

The *9/11 Commission Report* released in July 2004 highlighted the importance of information sharing as a foundational element necessary in the fight against terrorism. Many of the recommendations documented in the *9/11 Commission Report* were mandated in the *Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)*.

On August 3, 2007, the President signed the *Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act)*, which includes measures associated with IRTPA and enhances existing information sharing endeavors. Section 1203 of the Act requires that the Secretary of Homeland Security establish a Transportation Security Information Sharing Plan (TSISP) in consultation with the Program Manager of the Information Sharing Environment (PM-ISE), the Secretary of Transportation, and public and private stakeholders¹.

The TSISP is closely aligned and consistent with the overarching National Strategy for Information Sharing, the Information Sharing Environment Implementation Plan (ISE-IP), the National Infrastructure Protection Plan (NIPP) and the Transportation Systems Sector Specific Plan (TS-SSP). It will also be aligned with the DHS Information Sharing Strategy (dated May 12, 2008), which creates an essential link between the National Strategy and the ISE-IP and the TSISP and with TSA's sector-specific plans.

The purpose of the TSISP is to establish the steps necessary to build a foundation for sharing transportation security information between all entities that have a stake in protecting the Nation's transportation system - Federal, and State, local, and tribal (SLT) agencies and governments, the private sector, and foreign partners. Building on the progress of the past five years, implementing this plan will further improve the way in which we share information and fight terrorism.

1.2. Scope

This plan considers the full range of information sharing among the public and private sectors and leverages the progress already made to get the right information to the right people. It encompasses cross-domain information sharing, which is the sharing of highly sensitive and classified intelligence information and the more general sharing of unclassified information that improves an entity's ability to prevent, protect, deter and recover from a terrorist attack. Aligned with the framework of the Information Sharing Environment (ISE), this plan addresses the current state of transportation information sharing and the future direction of systems and processes.

1.3. Relevant Legislation & Guidance

Since the September 11, 2001, terrorist attacks, the U.S. Government has developed significant legislation, policy and guidance that establish the foundation for information sharing. Though most of the significant security legislation passed after September 11, 2001, addressed information sharing, IRTPA Section 1016 called for the creation of the ISE, and a PM-ISE with government-wide authority to plan, oversee and manage the ISE. The *9/11 Act*, Section 1203, requires DHS to establish a plan describing how intelligence analysts within DHS will coordinate with other Federal and SLT government agencies, as well as public and private stakeholders, to efficiently share transportation security information. Other key documents relevant to information sharing, including the DHS Information Sharing Strategy and the One DHS Memorandum, are discussed in Appendix (B)

¹ "The term 'public and private stakeholders' means Federal, State, and local agencies, tribal governments, and appropriate private entities, including nonprofit employee labor organizations representing transportation employees." From *Implementing Recommendations of the 9/11 Commission Act of 2007, Section 1203*.

1.4. Plan Coordination Process

As required by the 9/11 Act, TSA solicited input and coordinated this plan with the Department of Transportation, the PM-ISE, and other public and private stakeholders. Using the transportation sector partnership structure, the plan was coordinated with the Transportation Sector Government Coordinating Council (GCC) and the mode-specific Sector Coordinating Councils (SCC). All comments and inputs were considered in the final version of this document. The GCC will propose to the SCC establishing a joint Information Sharing working group to implement this plan and improve future versions. TSA will ensure that the plan and any future changes is reviewed through the DHS Information Sharing governance structure, and will continue to seek suggestions from all partners interested in information sharing for improving the information sharing process, which will be reflected in future updates to this plan.

2. Current State of Transportation Sharing

This section discusses some of the processes and environments that the transportation sector is currently using to share information. The current process is designed to communicate both actionable information on threats and incidents, and information pertaining to overall transportation sector status (e.g. plausible threats, vulnerabilities, potential consequences, incident situation, and recovery progress). This is accomplished through the collection, production and sharing of information, that enables timely and effective decision-making, so that owners and operators of critical infrastructure, SLT governments, and other security partners can assess risks, make appropriate security investments, and take effective and efficient protective actions.

Since its creation DHS has sought innovative and effective ways to share information with all stakeholders. DHS has consistently made effective communications and information sharing a pillar of its strategy and operational approach. Most strategic documents and plans on transportation security discuss the availability and flow of accurate, timely, and relevant information and/or intelligence about terrorist threats and other hazards, information analysis and incident reporting. Effective communication is a difficult task given the significant complexity of the transportation security network and the vast number of stakeholders that span Federal and SLT government agencies, as well as private entities and foreign partners.

2.1. Network Model

The Transportation System as a sector comprises all modes of transportation (i.e. aviation, maritime, mass transit, rail, highway, and pipeline) and is a vast, open, complex, and interdependent "networked" system that moves millions of passengers and goods. Disruptions in the transportation network can often have non-linear effects. As a result, what may initially appear as an isolated disturbance in the network can have a much greater impact within and beyond the sector.

In response, DHS's information sharing approach constitutes a shift from a strictly hierarchical model to one reflecting the networked nature of the sector. It allows for distribution and access to information both vertically and horizontally, as well as the ability to enable decentralized decision making and actions.

The Transportation Security Administration (TSA) was established with a mandate that includes responsibility for the security of the Nation's transportation systems. Within TSA each mode of transportation is organized under a single primary Point of Contact (POC), or a General Manager (GM) uniquely positioned for the sharing of transportation security information with public and private stakeholders. These GMs, many of whom are senior executives with significant experience in the sector for which they are responsible, chair their respective GCC and are responsible for managing interactions with other Federal, SLT, and private sector entities. The Table below identifies how the network leads are organized by mode of transportation.

228

Transportation Mode		General Manager
Aviation	Airlines	David Bernier
	Airports	Douglas Hofsass
	Air Cargo	Edward Kelly
	General Aviation	Michal Morgan
Highway		William Arrington
Freight Rail		Gilbert Kovar
Maritime (USCG)		Dana Goward
Mass Transit		Paul Lennon
Pipeline		Jack Fox

Modal Points of Contact

229

2.2. Current Information Sharing

230

231 Information sharing is a multi-directional activity that occurs informally through relationships and more formally
 232 through communication policies, regulations, procedures, guidance and tools. Intelligence and information
 233 sharing are at the core of the overall transportation security strategy. The primary mechanisms for the sharing of
 234 transportation security information and the coordination of intelligence activities can currently be categorized into
 235 four general areas:

- 236 1. **Information Sharing Environment.** IRTPA Section 1016 requires the Federal Government to create an
 237 ISE for the sharing of terrorism information in a manner consistent with national security and with
 238 applicable legal standards relating to privacy and civil liberties. The ISEIP defines the Federal
 239 Government's information sharing strategy and provides the building blocks needed to successfully
 240 implement an ISE.

241 In alignment with the PM-ISE, DHS is establishing its ISE, and has established a governance structure
 242 through the Information Sharing Governance Board (ISGB) and the Information Sharing Coordinating
 243 Council (ISCC), in which TSA full member. Additionally, TSA has taken significant initial steps in
 244 establishing a Transportation ISE, in alignment with the PM-ISE and DHS ISE, to provide the right
 245 information to the right people, at the right time, through collaboration within and across the
 246 transportation sector network. DHS and its transportation security stakeholders have focused on the core
 247 mission capabilities needed to maximize information sharing as identified by the Program Manager. DHS
 248 has begun by building the necessary foundation to provide these mission capabilities internally so it will
 249 be better equipped to support these capabilities across the transportation network in the future.

250 Part of the Transportation ISE is TSA's system of Web Boards and sharing of homeland security and
 251 terrorism information with regulated and unregulated stakeholders. For regulated aviation stakeholders,
 252 for example, security programs are shared with and between TSA and appropriate stakeholders to
 253 develop, approve and amend these crucial Sensitive Security Information (SSI) documents. SSI is
 254 appropriately shared and protected within the Transportation ISE in accordance with Title 49 of the Code
 255 of Federal Regulations, part 1520 (49 CFR 1520).

- 256 2. **Office of Intelligence.** TSA is the Department lead on transportation-related intelligence and analysis.
 257 TSA's intelligence mission is to provide timely and accurate intelligence and information related to
 258 threats to transportation; this information is provided to TSA, DHS' Office of Intelligence and Analysis
 259 (I&A), DHS leadership and field entities, and other Federal and SLT authorities, as well as foreign

partners. TSA functions as the operational conduit between the public and private transportation security stakeholders and the Intelligence Community (IC), and is a full partner with other DHS intelligence components. TSA is a member component of the DHS Intelligence Enterprise, which is led and managed by the Department's Chief Intelligence Officer (CINT).

3. **Sector Partnership Model.** DHS uses the transportation sector partnership, specifically the GCC and SCC structures as the primary mechanism to coordinate transportation information sharing policy, strategy, plans, issues and requirements development. Coordination with the DHS's information sharing coordinating bodies will also be ensured.
4. **Transportation Security Operations Center (TSOC).** A sophisticated 24-7 operations center that maintains continuous information sharing with Federal, State, local, tribal and private transportation-related entities. It serves as the main POC for security-related incidents or crises in all modes of transportation and is the primary interface to the DHS National Operations Center (NOC) for these incidents or crises. The TSOC's mission is to coordinate and communicate intelligence and domain awareness information for U.S. transportation related security activities worldwide. Its strategic goals are incident prevention and/or interdiction, threat mitigation and incident coordination and management.

Today, building on the efforts of transportation partners in the IC, DHS uses intelligence and analysis to prioritize security activities. Each day begins with briefings on the latest intelligence from the IC and that information drives the decision making process both operationally and strategically. In addition, DHS shares intelligence and information as appropriate with governmental partners and sector stakeholders for further dissemination to appropriate operating and security officials and front-line employees enabling them to make informed security decisions. Specific examples include:

- The Homeland Security Information Network (HSIN) includes mode-specific portals, such as Mass Transit, Highway, and Pipeline portals, providing one-stop security information sources and outlets for security advisories, alerts and notices. The modal portals afford stakeholders not only access to current information, but also networking capabilities for information sharing among themselves. Additionally, TSA modal divisions have the ability to maintain web pages on the TSA public site to provide information on security strategies, priorities and programs.
- The Highway and Motor Carrier Industry Information Sharing and Analysis Center (ISAC) and the Highway Watch® program are active and continually processing reports from highway operators and sharing information between industry and DHS.
- The Public Transit ISAC communicates security-related information and advisories obtained through open and secure sources to over 400 public transit systems.
- The DHS Alert system has delivered over 1.4 million alerts to more than 10,000 DHS users with activities currently underway to extend support to external transportation stakeholders (i.e. Federal, SLT, and commercial) as well. These included a substantial number of useful alerts containing general information not directly pertinent to terrorist threats.

3. Transportation Security Information Sharing

The TSISP builds upon existing transportation security information sharing regulations, initiatives, resources and tools to strengthen the foundation of a shared mission community. By combining people, processes, and technology, information will be created and shared so that terrorism is prevented, the U.S. and international transportation network is secured, and the free flow of people and commerce occurs.

Leveraging the progress and the mechanisms that are already in place, the transportation security components of the DHS ISE will support the sharing of transportation security information across multiple stakeholders including Federal and SLT government agencies, and other public and private entities. This approach will promote collaboration and coordination among all of the transportation security stakeholders. The collaborative

effort enables DHS to provide “High Value” information, ultimately protecting the transportation network against terrorism while ensuring freedom of movement of people and commerce.

3.1. Defining our Goals

Successful information sharing is an underlying requirement for achieving DHS’s strategic goals. DHS’s information sharing goals, derived from the ISE-IP, focus on effectively sharing transportation security information in order to maintain the security of the national and international transportation network, but also to address the recommendations from the *9/11 Commission Report*. Goals for the sharing of transportation information are:

- **Multi-Directional Sharing:** Establish a framework enabling secure, multi-directional transportation security information sharing between government and industry
- **Effective and Efficient Processes:** Establish clear governance, roles, responsibilities, and communication protocols between transportation security stakeholders to promote more rapid and effective exchange of information, analysis, and coordination
- **Trusted Partnership:** Establish trusted partnerships among all levels of the transportation security network
- **Right Information-Right People-Right Time:** Improve the timely and secure exchange of transportation security information supported by education, training, awareness programs, and enabling technologies
- **Protect Privacy and Civil Liberties:** Ensure privacy and civil liberties are protected within the transportation security network

3.2. Guiding Principles

In order to successfully implement the TSISP, TSA must take several steps to develop the principles and lay the foundation for improved information sharing. These key activities guide the plan’s framework, capabilities and adoption elements:

- **Align with PM-ISE:** Continue to align itself with the DHS-ISE to ensure its strategy meets the overarching information sharing mission and must continue to coordinate with DHS’s governance structure, specifically the ISGB and ISCC.
- **Align with the DHS Intelligence Enterprise:** Coordinate and consolidate transportation analysis and produce intelligence products and alerts by applying formats and standards established by the CINT and using all-source intelligence and information provided by the DHS Intelligence Enterprise.
- **Coordinate with Stakeholders:** To understand mission challenges and specific needs for information sharing services, reach out to potential stakeholders within DHS, as well as to other Federal and SLT communities. From a governance perspective, continue to grow existing Information Sharing Coordination Councils into mature committees including establishing relevant and timely transportation security working groups and Communities of Interest (COI), ensuring appropriate coordination with the DHS information sharing coordinating structures.
- **Conduct Stakeholder Prioritization:** Based on regulatory requirements, and operational and mission goals, certain stakeholder groups will benefit more than others from access to transportation security information. Whether inside DHS, the Federal Government in general, within specific SLT agencies, or the private sector, the stakeholders that have a more pressing need for information related to transportation security will be considered priority recipients of information sharing services because, for example, they operate or protect transportation systems or assets at greater risk and need to take more immediate action. TSA will assess private sector stakeholders on an individual basis, as they establish themselves as relevant consumers of transportation security information.
- **Conduct Requirements Analysis:** Conduct fit-gap analysis sessions with prioritized stakeholders in order to gather requirements for future information sharing services.

- **Develop and Implement Information Sharing Services:** Based on requirements gathered for prioritized stakeholders, implement information sharing services related to transportation security; leverage existing services previously developed (e.g. DHS Alert) wherever possible; as needed, design, develop and implement services that address core mission challenges.
- **Expand Mission Capabilities:** Deliver mission capabilities to external stakeholders as prioritized by the governing bodies as established by the TSISP.
- **Refine Existing Mechanisms:** Use lessons learned to further refine the implementation methodology to deliver mission capabilities more efficiently and increase mission user adoption of information services.

3.3. Information Sharing Environment Framework

3.3.1. PRIVACY

While the *9/11 Act* emphasizes the need for information sharing, it also stresses the importance of protecting information privacy and civil liberties. The TSISP will be consistent with the privacy guidelines for information sharing as defined in the PM-ISE's ISE-IP and the designated DHS ISE Privacy Official will work in consultation with the Privacy and Civil Liberties Oversight Board, established under section 1061 of IRTPA.

3.3.2. SECURITY

Sharing information within and outside the Federal Government can become extremely complicated depending on the classification of the information being shared. The goal is to create solutions that will allow, to the greatest extent possible, information to be exchanged across the three security domains shown in Figure 1: Unclassified, Secret, and Top Secret. DHS will follow the direction and policies defined by the PM-ISE to address this complex problem.

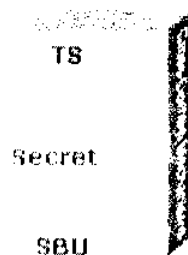


Figure 1: Security Domains (PM-ISE Implementation Plan, Figure 3.6-1)

TSA will implement the PM-ISE's cross-domain mechanism to facilitate sharing and coordination between different classification levels, including:

- **Standardization:** Continuing to use SSI as a statutory-based SBU regime will build on its current familiarity to the transportation stakeholders. These users will occasionally encounter other types of SBU, however, so standardizing procedures and requirements for designating, marking, handling and safeguarding non-regulatory SBU information across the Federal, SLT, and law enforcement agencies, and private sector entities will further support simplified sharing. DHS also plans an education and outreach effort to transportation and other sector stakeholders to explain the standardized regime.
- **Tearlines:** Tearlines that enable the flow of information to lower security domain by extracting portions shareable at that level.
- **Controlled Interface:** Controlled interfaces that provide automated, secure, two-way transfer of information between domains.

- **Identifiers:** Information identifiers that inform users will be made available, as appropriate. When not appropriate, the recipient will be informed why the identifiers are not available as well as the fact the information exists, but is unavailable.
- **Authorities:** Proxies that may be used by higher-level domain users to access services at a lower level domain while complying with domain security requirements.
- **Messaging:** Organizational messaging that ensures a trusted exchange of organizational electronic messages between two domain levels.

In addition, DHS personnel continue to work with key stakeholders to identify those officials that need clearances, the appropriate level of clearance, and the best process in which to obtain a clearance.

3.4. Adoption of the Information Sharing Environment

3.4.1. SHARING INFORMATION AT THE FEDERAL LEVEL

DHS continues to share transportation security information with other Federal Government partners through the organizational constructs delineated in this plan. This includes, but is not limited to, the ISE, the Interagency Threat Assessment and Coordination Group, and the NIPP and corresponding TS-SSP.

Additionally, as Federal partners develop information sharing strategies specific to their mission and operational goals, DHS will look to collaborate with these groups in an effort to leverage existing information sharing plans, minimize duplicative documentation, and maximize returns from information sharing investments. This collaborative approach at the Federal level will in turn drive the manner in which terrorism-related information is shared with non-Federal partners.

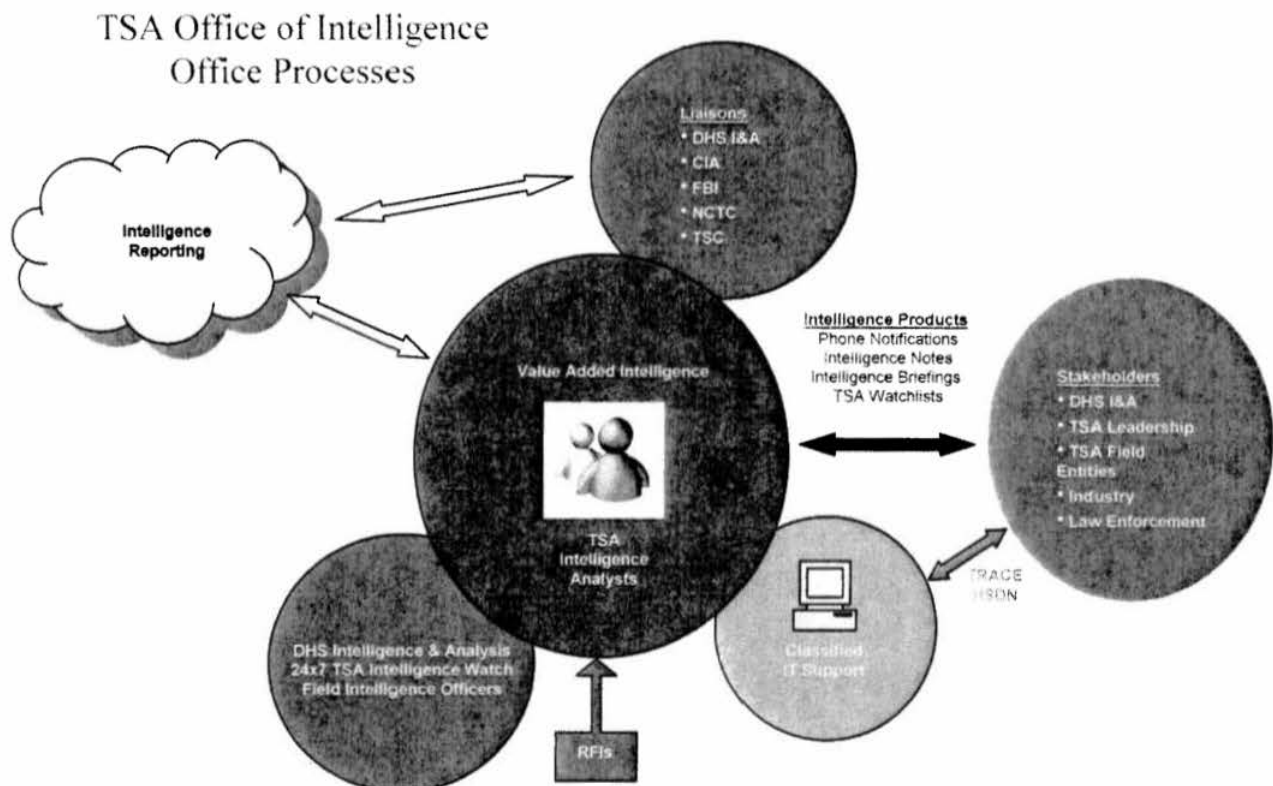


Figure 2: Intelligence Reporting Process

Within DHS, TSA serves as the primary transportation security liaison to the intelligence and law enforcement communities. As shown in Figure 2, TSA's intelligence mission is to provide timely and accurate intelligence

and information related to threats to transportation to TSA and DHS leadership, field entities, and other Federal and SLT authorities. In support of TSA's mission, the TSOC integrates information provided by TSA-Intel, fusing together actionable intelligence with operational information across all modes of transportation.

DHS uses technologies, consistent with the ISE, to communicate cross-domain (i.e., classified and unclassified) information with its Federal partners, including:

- **Joint Worldwide Intelligence Communications System (JWICS):** A system of interconnected computer networks used to transmit classified information in a secure environment.
- **INTELINK:** A highly secure intranet used by the U.S. IC. It serves as the web environment on protected top secret, secret and unclassified networks.
- **Homeland Secure Data Network (HSDN):** Functioning as DHS's secure communications infrastructure, it allows Federal and SLT governments to share timely and actionable classified information. HSDN is a full service system, that provides user agencies the workstations, applications, and help desk support needed to achieve superior intelligence communication. It is the major secure information thoroughfare joining together intelligence agencies, law enforcement, disaster management and front-line disaster response organizations in the common goal of protecting our Nation and its citizens.
- **Secret Internet Protocol Router Network (SIPRNet):** A system of interconnected computer networks used to transmit classified information in a secure environment.
- **Non-secure Internet Protocol Router Network (NIPRNet):** Used to exchange sensitive but unclassified information between internal users as well as providing user access to the Internet.
- **TSA Remote Access to Classified Enclaves (TRACE):** A high-speed, National Security Agency-approved system designed to quickly and securely provide remote TSA field locations with classified and unclassified intelligence information. Currently this system supports up to the Secret Collateral security level.
- **TSA Automated Inspections, Enforcement, and Incident Reporting Subsystem.** This system supports a broad range of mission requirements to include data capture of critical records documenting security compliance and oversight inspections; outreach contacts with industry stakeholders; administrative enforcement and regulatory investigations; and the details and the subjects associated with reported security incidents. This enterprise application serves more than 5,000 authorized internal users and is part of the agency's information technology enterprise. Data outputs from this accredited application are used to support external Freedom of Information Act requests, internal operations research, and out-of-agency requests for transportation security statistics. Planned strategic expansion of the application will accommodate a growing enterprise and will facilitate the swift exchange of data and analysis. Currently housing more than a million individual subject name records, alone, this application also augments the critical functions performed by the several organizational elements mentioned in Section 2.2, namely the Office of Intelligence, the Sector Partnership Model, and TSA's 24/7 operations center.

TSA also provides information through a variety of intelligence products, which are delineated in the Appendix (C) to this plan.

3.4.2. SHARING INFORMATION WITH STATE, LOCAL AND TRIBAL GOVERNMENTS

SLT authorities are critical to our Nation's efforts to prevent future terrorist attacks and are the first to respond if an attack occurs. These governments carry out their counterterrorism responsibilities within the broader context of their core mission to protect the public's health and safety and to provide emergency and non-emergency services. DHS has an integrated approach that allows Federal agencies to work together to produce and disseminate terrorism information. This includes:

- **Fusion Centers:** DHS and the ISE support the SLT governments by providing analysts and direct support to establish State and major urban area information fusions centers. These centers work toward

the common goal of blending relevant law enforcement and intelligence information analysis and coordinating security measures to reduce threats in their communities. Fusion centers serve as the primary focal points with these environments for the receipt and sharing of terrorism-related information, and play a vital role in disseminating terrorist information at the state level. DHS supports these centers through grant funding, technical assistance, training; and by deploying departmental officers and intelligence analysts to fusion centers nationwide to achieve a baseline level of capability.

- **Joint Terrorism Task Forces (JTTF):** DHS has a significant presence in the JTTF in major cities throughout the United States. TSA's Federal Air Marshal Service has representatives on all 56 major Federal Bureau of Investigations Field Office JTTFs and several of its resident office JTTFs. These have substantially contributed to improved information sharing and operational capabilities at the State and municipal levels.

3.4.3. SHARING INFORMATION WITH THE PRIVATE SECTOR

Private industry within the transportation sector has made significant investments in mechanisms and methodologies to evaluate, assess, and exchange information across regional, market and security-related COIs. DHS continues to work with the private sector to build on these efforts to adopt an effective framework that ensures a two-way flow of timely and actionable security information between public and private partners. DHS has established several information sharing mechanisms to disseminate and receive information with the private sector. These include:

- **Critical Infrastructure Partnership Advisory Council:** CIPAC directly supports DHS's sector partnership model by providing a legal framework for members of the GCC and Sector Coordinating Council to collaborate on a broad spectrum of security activities. This approach aligns with the NIPP and the corresponding TS-SSP, the ISE-IP and other information sharing guidance. The SCC plays an important role in providing the private sector perspective on identifying and implementing the information sharing mechanisms that are most appropriate for their mode of transportation.
- **Homeland Security Information Network:** DHS communicates in real-time to its partners by utilizing the internet-based HSIN. System participants include governors, mayors, Homeland Security Advisors, State National Guard offices, Emergency Operations Centers, First Responders and Public Safety departments, and other key homeland security partners. The system is a highly secure network with a common set of information-sharing functions and tools for various private sector communities with common security interests. It is sponsored by DHS and managed by the private sector-led SCC and/or its designees. The mode specific sub-portals are currently in various stages of development, with three modes of transportation – Mass Transit, Highway and Motor Carrier, and Pipeline, with fully functioning portals.
- **Information Sharing and Analysis Centers:** These entities play a vital role in facilitating communication and coordination of information related to terrorism. DHS continues to operationally coordinate and work with transportation industry ISACs daily to address security issues. Various ISACs have access to and work with the TSOC, and with TSA's modal experts and intelligence personnel. ISAC personnel have access to information and intelligence consistent with security policies.
- **Homeland Infrastructure Threat and Risk Analysis Center (HITRAC):** HITRAC is the national infrastructure integration center for threat and risk. This office, jointly resourced by the DHS Office of Infrastructure Protection and DHS I&A, provides primary, collaborative, and integrative tactical and strategic intelligence and assessments of threats to the nation's critical infrastructure. HITRAC develops intelligence products to help inform State and Local Fusion Centers (SLFC) and infrastructure owners and operators of any threats they may potentially face, as well as to better inform their security planning and investment decisions.

HITRAC integrates the intelligence assessments with assessments of infrastructure vulnerabilities and consequences to provide sector and comprehensive national assessments of risk. HITRAC collaborates with TSA for intelligence assessments and uses transportation threat and risk assessments to inform

assessments of other sectors based on dependencies on transportation. HITRAC is the lead for establishing and coordinating support to SLFC, including sharing intelligence and information sharing, and provides the threat assessments for annual grants and responses to the state and UASI city assessments. HITRAC also leads cyber intelligence analysis and provides inter-dependency threat and risk assessments, including transportation dependencies.

- **National Infrastructure Coordination Center (NICC):** Serves as an extension of the NOC, providing the mission and capabilities to assess the operational status of the Nation's Critical Infrastructures and Key Resources, supports information sharing with the ISACs and the owners and operators of critical infrastructure facilities, and facilitates information sharing across and between the individual sectors.
- **Sensitive Security Information (SSI):** This statutory and regulatory-based framework for transportation security-related SBU information allows streamlined and safe sharing of such information with State, local and tribal governments, law enforcement, and private industry to enhance transportation security.
- **Protected Critical Infrastructure Information Program (PCII):** This statutory and regulatory-based framework enables the private sector to voluntarily submit sensitive information regarding the Nation's critical infrastructure to DHS with the assurance that the information, if it meets certain requirements, will be protected from public disclosure. The program seeks to facilitate greater sharing of critical infrastructure information among the owners and operators of the critical infrastructures and government entities with infrastructure protection responsibilities, thereby reducing the Nation's vulnerability to terrorism.
- **DHS Protective Security Advisors (PSA):** To better partner with SLT governments, and the private sector, DHS has deployed a cadre of highly-experienced security specialists in regions throughout the country to assist local efforts to protect critical assets and provide a local perspective to the national risk picture. With significant experience in emergency management, these dedicated critical infrastructure and vulnerability assessment experts, or PSAs, are recruited from, live, and work in these communities. They provide a federally funded resource to communities and businesses to assist in the protection of critical assets.

3.4.4. SHARING INFORMATION WITH THE FOREIGN PARTNERS

The sharing of terrorism-related information between Federal departments and agencies and foreign partners and allies forms a critical component of our information sharing strategy. After the September 11 attacks, many foreign governments joined us in declaring war on terrorism and have since contributed in important ways. Intelligence provided by foreign partners often provides the first indications of terrorist plans and intentions. Accordingly, we will enhance standards and provide more capabilities for improved sharing with our foreign partners and allies.

In addition to receiving such information from other countries, it is also critical that we appropriately share similar types of information with foreign governments or foreign law enforcement entities, such as INTERPOL. In doing so, we must ensure that any sharing of any records about American citizens and lawful permanent residents is in compliance with U.S. privacy rights and protections.

TSA recently realigned to create an Office of Global Strategies with the mission of increasing security by working proactively with our foreign partners and overseas operations affecting the United States. The agency has been able to significantly strengthen its relationships with international transportation security partners through increased communications, information sharing, and best practices. Examples of international cooperation that the Office of Global Strategies aims to increase and strengthen include common strategies on screening liquids, aerosols, and gels and implementing advanced technologies and intelligence sharing.

Other activities include:

- **European Union Passenger Name Record Agreement:** The United States and the European Union have agreed to a security program that shares personal data about millions of United States-bound airline passengers a year. Under the agreement, airlines flying from Europe to the United States are required to

provide data related to these matters to U.S. authorities if it exists in their reservation systems. The agreement allows DHS to retain and use it "where the life of a data subject or of others could be imperiled or seriously impaired," such as in a counterterrorism investigation.

- **Transportation Security Administration Representatives (TSARs):** These personnel serve as official TSA representatives around the world. TSARs are located in foreign countries and work closely to share information with their governments to improve international transportation security. TSA also has an experienced corps of aviation security experts based internationally with regulatory and inspection responsibility that also share information. Their talents can meaningfully increase security measures in cooperation with airlines and other governments.

3.5. Specific Implementation Actions

As stated above, DHS has aligned its strategy with the PM-ISE and will therefore participate in the primary and most applicable implementation activities identified by the PM-ISE in its Implementation Plan. Specifically, the following table identifies implementation actions specific to the sharing of transportation security information between all relevant stakeholders.

Action Number	Action
Framework – Program management and governance activities as well as infrastructure components required to support the information sharing framework such as hardware, software, data centers, networking and security controls.	
1.1	Coordinate with DHS. TSA will coordinate with DHS, its information sharing governance structure and strategy, and its efforts to create a DHS-ISE, to include coordinating with DHS ISGB and ISCC.
1.2	Align with PM-ISE. Align with the PM-ISE to ensure that the overarching information sharing mission is consistent with the DHS's transportation security strategy. Alignment includes following PM-ISE's governance, architecture and standards, and information privacy guidelines.
1.3	Coordinate with Stakeholders. To understand mission challenges and specific needs for information sharing services, reach out to potential stakeholders within DHS, as well as to other Federal and SLT communities; continue to grow existing ISCC's into mature committees including the establishment of relevant and timely transportation security sub-committees, working groups and COIs; develop education and training programs in order to improve the sharing of information between the private sector and the public sector.
1.4	Fully establish the Transportation Security Information Sharing Coordination Council (TS-ISCC). Establish the ISCC to create or adopt all relevant policies and procedures and prioritize technology investments.
Capabilities - Development of services within the six core capability areas in support of the transportation information sharing mission.	
1.5	Conduct Stakeholder Prioritization. Identify stakeholders operating in higher risk areas that may have a more pressing need for information related to transportation security for consideration as priority recipients of information sharing services
1.6	Conduct Requirements Analysis. Conduct requirements gathering sessions with stakeholders to identify and prioritize key transportation security information sharing gaps.
1.7	Prioritize Capabilities. The Transportation Security ISCC will prioritize the mission capabilities to be implemented across all security domains (i.e., SBU, Secret, Top Secret) and the overall adoption approach for appropriate public and private stakeholders.
1.8	Identify Reusable Technologies. DHS, in conjunction with its transportation security stakeholders will investigate existing or emerging technologies that can be leveraged to expedite the implementation of mission capabilities.
1.9	Develop and Implement Information Sharing Services: Based on requirements gathered for prioritized stakeholders, implement information sharing services related to transportation security; leverage existing services previously developed (for example, DHS Alert)

Action Number	Action
	wherever possible; as needed, design, develop and implement services that address core mission challenges.
1.10	Implement Capabilities for the SBU Domain. Based on the ISCC's prioritization, DHS will implement transportation security mission capabilities in the SBU domain.
1.11	Implement Capabilities for the Classified Domains. Based on the ISCC's prioritization, DHS will implement transportation security mission capabilities in the classified domains (i.e., Secret, Top Secret).
1.12	Refine Existing Mechanisms. Use lessons learned from the existing internally-focused capability implementations to further refine the adoption methodology to deliver mission capabilities more efficiently.
Adoption - Rolling capabilities out to transportation security public and private stakeholders.	
1.13	Sharing with Federal Partners. DHS will coordinate with other Federal Partners directly, as part of the PM-ISE ISC, and as part of the Transportation GCC to prioritize adoption of relevant information sharing capabilities across the Federal Government.
1.14	Sharing with SLT Governments. DHS's State and Local Program Management Office (SLPMO) and TSA will coordinate to determine the prioritization of SLFC for deployment of information sharing capabilities as well as operational and intelligence personnel. Additionally, DHS will follow the PM-ISE framework for sharing information beyond the Federal Government and will coordinate with the Transportation GCC.
1.15	Sharing with the Private Sector. DHS will coordinate with the mode-specific SCCs to determine prioritization for deployment of information sharing capabilities to private sector organizations with transportation security responsibilities.

566 4. Resources and Schedule

567

568 4.1. Resource Estimates

569 To date TSA expended approximately \$20 million of base funding over 3 years on ISE development. Further
 570 development and implementation, subject to future funding, will occur in multiple-phases over a period of several
 571 fiscal years. Initial activities will focus on the expansion of mission capabilities within DHS and the foundational
 572 components necessary to expand mission services to other Federal agencies. Subsequent phases will result in the
 573 deployment of mission capabilities to Federal, SLT, and private sector stakeholders, in addition to the
 574 continuation of advancements in DHS and Federal workspaces.

575 4.2. Implementation Schedule

576 The TSISP is currently implemented at an initial operating capability. There is a high-level of information
 577 sharing occurring on a regular basis. This plan provides a more formal and repeatable framework for information
 578 sharing. The implementation of this framework relies on continued coordination with the PM-ISE and
 579 stakeholders to further define requirements and prioritize available resources. TSA expects that full
 580 implementation could occur over several years in multiple phases (development, enhancement/refinement, and
 581 operations and maintenance).

582

Appendix (A)

List of Acronyms

The following acronyms are used in this document:

9/11 Act	Implementing Recommendations of the 9/11 Commission Act of 2007
ADIB	Administrator's Daily Intelligence Briefing
CATA	Cities & Airports Threat Assessment
CIPAC	DHS Critical Infrastructure Partnership Advisory Council
COI	Communities of Interest
CTIP	Collaborative Transportation Imagery Project
DHS	Department of Homeland Security
DHS I&A	DHS Office of Intelligence and Analysis
FIO	Field Intelligence Officers
GCC	Transportation Sector Government Coordinating Council
GM	General Manager
HIR	Homeland Intelligence Report
HITRAC	Homeland Infrastructure Threat and Risk Analysis Center
HSDN	Homeland Secure Data Network
HSIN	Homeland Security Information Network
IC	Intelligence Community
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
ISAC	Information Sharing and Analysis Center
ISCC	Information Sharing Coordination Councils
ISE	Information Sharing Environment
ISE-IP	Information Sharing Environment Implementation Plan
JTTF	Joint Terrorism Task Forces
JWICS	Joint Worldwide Intelligence Communications System
NCTC	National Counterterrorism Center
NICC	National Infrastructure Coordination Center
NIPP	National Infrastructure Protection Plan
NIPRNet	Unclassified but Sensitive Internet Protocol Router Network
NOC	DHS National Operations Center
PCII	Protected Critical Infrastructure Information Program
PM-ISE	Program Manager of the Information Sharing Environment
POC	Point Of Contact
PSA	Protective Security Advisors
SBU	Sensitive But Unclassified
SCC	Mode-specific Sector Coordinating Councils
SIPRNet	Secret Internet Protocol Router Network
SIR	Suspicious Incidents Report
SLFC	State and Local Fusion Centers
SLPMO	State and Local Program Management Office
SLT	State, Local, and Tribal
SSI	Sensitive Security Information
TIG	Transportation Intelligence Gazette
TRACE	TSA Remote Access to Classified Enclaves
TSA	Transportation Security Administration
TSA-Intel	TSA Office of Intelligence
TSAR	Transportation Security Administration Representatives
TS-ISCC	Transportation Security Information Sharing Coordination Council

Transportation Security Information Sharing Plan

TSISP	Transportation Security Information Sharing Plan
TSOC	Transportation Security Operations Center
TS-SSP	Transportation Systems Sector Specific Plan
WFIS	Weekly Field Intelligence Summary

588

Appendix (B)

Relevant Legislation & Guidance

Key documents relevant to the foundation of information sharing are listed below:

- *Aviation Security Improvement Act of 1990*, dated November 16, 1990. This Act underscores the operational aviation security regulations (49 CFR parts 1542, 1544, 1546, 1548, etc.) that govern the sharing of SSI with airports, airlines, air cargo forwarders, and other domestic and foreign stakeholders.
- *49 CFR part 1520. Sensitive Security Information*, dated February 22, 2002. This Federal regulation outlines policies and procedures in how to share, safeguard, and identify sensitive transportation security information that is shared with transportation security stakeholders.
- *Protecting America's Freedom in the Information Age*, dated October 7, 2002. Published by the Markle Foundation's Task Force, this report stresses the importance of information in the war on terrorism. It defines a holistic approach to information sharing and sets forth recommendations for enhancing the manner in which information is collected and analyzed to improve the Nation's preparedness against terrorist attacks. In its second report, entitled *Creating a Trusted Network for Homeland Security*, dated December 2, 2003, the Task Force reiterates the importance of information sharing. The report emphasizes the importance of creating a decentralized ISE as a top priority for the defense of the homeland. The report concludes that by using currently available technology, the government can set up a network that improves our ability to prevent terrorist attacks and protect civil liberties.
- *Homeland Security Act of 2002*, Pub. L. 107-296, 116 Stat. 2135, dated November 25, 2002. It established DHS by combining components from over 20 Federal agencies. The Act also mandated the adoption of information sharing procedures in order to protect the United States from terrorism.
- Executive Order 13354 - *National Counterterrorism Center*, dated August 27, 2004. This order established the National Counterterrorism Center (NCTC) as the "primary organization in the United States Government for analyzing and integrating all intelligence possessed or acquired by the U.S. Government pertaining to terrorism and counterterrorism.
- Executive Order 13356 - *Strengthening the Sharing of Terrorism Information To Protect Americans*, dated August 27, 2004. This order is aimed at strengthening the sharing of terrorism information to protect Americans. It directs agencies to give the "highest priority" to the prevention of terrorism and the "interchange of terrorism information [both] among agencies" and "between agencies and appropriate authorities."
- *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA), Pub. L. 108-458, 118 Stat. 3638, dated December 17, 2004. This act established the Office of the Director of National Intelligence, the Director of National Intelligence and a Program Manager. Section 1016 of the law stipulated that the PM will lead the development of an "Information Sharing Environment" that will coordinate terrorist information across the intelligence and law enforcement communities.
- Executive Order 13388 - *Further Strengthening the Sharing of Terrorism Information to Protect Americans*, dated October 25, 2005. This order established the Information

- 634 Sharing Council, chaired by the PM-ISE, who subsequently assumed responsibility for
635 the "establishment of an interoperable terrorism information sharing environment to
636 facilitate automated sharing of terrorism information among appropriate agencies."
- 637 • *Information Sharing Environment Implementation Plan*, dated November 2006. This
638 plan defined the Federal Government's information sharing strategy. It provides the
639 building blocks needed to successfully implement an ISE, and the roadmap that the PM-
640 ISE intends to follow.
 - 641 • *DHS Policy for Internal Information Exchange and Sharing*, dated February 1, 2007.
642 Known as the "One DHS" memo, this document instructs that DHS Components are
643 considered a single, united agency for information sharing purposes. The memo also
644 directs that all DHS employees should "have timely access to all relevant information
645 they need to successfully perform their duties", promoting a culture of information
646 sharing.
 - 647 • *Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act)*, Pub. L.
648 110-53, 121 Stat. 266, dated August 3, 2007. The Act implements many of the
649 recommendations of the 9/11 Commission and requires the Secretary of DHS to establish
650 the TSISP. Pursuant to the Act, the TSISP must describe how intelligence analysts
651 within DHS will coordinate with other Federal and SLT government agencies, as well as
652 public and private stakeholders, to efficiently share transportation security information.
 - 653 • *Homeland Security Information Technology Network Architecture Progress Report*,
654 dated October 29, 2007. This document reports on the progress made in implementing a
655 comprehensive information technology network architecture for the DHS Office of
656 Intelligence and Analysis that connects the various databases and related information
657 technology components of DHS in order to promote internal information sharing among
658 the intelligence and other personnel of DHS.
 - 659 • *National Strategy for Information Sharing – Successes and Challenges in Improving
660 Terrorism-Related Information Sharing*, dated October 31, 2007. This strategy
661 prioritizes and unifies our Nation's efforts to advance the sharing of terrorism-related
662 information. It sets forth a plan to build upon the progress made in improving
663 information sharing since the September 11, 2001, attacks and establishes an integrated
664 National information sharing capability. It was developed using a collaborative process
665 and based on significant input provided by members of the Federal Information Sharing
666 Council, as well as State, local, tribal, and private sector officials from across the Nation.
 - 667 • *DHS Information Sharing Strategy*, dated May 12, 2008. This strategy strives to
668 transform DHS into an organization whose culture, business processes, and governance
669 structure foster an information sharing environment that ensures the right information
670 gets to the right people at the right time.

Appendix (C)

Intelligence and Information Sharing Products

The TSA Office of Intelligence (TSA-Intel) operates a 24-7 indications and warnings watch. The Watch is connected to the IC and DHS I&A via JWICS, HSDN and SIPRNET, which provide the watch with access to both intelligence reporting from the field and finished intelligence products, including assessments. The headquarters watch has real-time access and contact with all U.S. IC Watches and operations centers. This access allows TSA-Intel to receive and provide real and near real-time intelligence on threats to the U.S. transportation system.

TSA-Intel provides detailed value added analytical products, in the form of classified and unclassified briefings, assessments, and summaries. These products are presented to TSA/DHS leadership, SLT authorities and law enforcement, TSA field entities and representatives, foreign officials and private sector stakeholders. Under the 49 CFR 1500 series, TSA may issue an Information Circular to notify stakeholders about security concerns. When TSA determines the additional security measures are necessary to respond to a threat assessment or to a specific threat against civil aviation, TSA issues a Security Directive setting forth mandatory measures.

TSA-Intel also has Field Intelligence Officers (FIOs) at airports around the United States. The FIOs interact with TSA officials, other Federal agencies and SLT officials in areas to which they are assigned. They are the face of TSA-Intel for all intelligence support and activities outside of the Washington D.C. area.

TSA provides the following intelligence and information sharing products to partners and stakeholders on a routine basis:

- **Administrator's Daily Intelligence Briefing (ADIB).** A 24-hour snapshot of transportation-related intelligence comprised of TSA operational and Intelligence Community reporting. This product is disseminated through TRACE and classified e-mail to a limited TSA audience.
- **Transportation Intelligence Gazette (TIG).** The TIG, usually a classified analytic document, aims to bridge the gap between the ADIB and modal threat assessments by providing in-depth analysis focused on a specific topic within a transportation mode. The document may also be used to provide additional information or background on an issue, or to provide situational awareness. TIG lengths vary and are disseminated through TRACE, NCTC Online, HSIN Intel, HSDN, and classified and unclassified email lists.
- **Suspicious Incidents Report (SIR).** The SIR provides a weekly summary and analysis of operational reporting on suspicious activities and surveillance directed against all transportation modes. Sources for the SIR include law enforcement (LE) and IC reporting. This product is available in both classified and SSI editions and is disseminated via multiple LE and IC distributions lists, portals, and Web boards.
- **Weekly Field Intelligence Summary (WFIS).** The WFIS is a weekly analytical summary of law enforcement and open source reporting produced at the SSI level. The document provides information on threats, significant airport and aircraft incidents, and IC and LE advisories. The WFIS is disseminated via a Sensitive Security Information (SSI) distribution list and posted on LE and IC portals and Web boards.
- **Cities & Airports Threat Assessment (CATA).** The CATA is a classified and SSI-level domestic and overseas flight risk assessment provided to TSA International, Federal

- 715 Air Marshals, and Airport Security Inspectors to assist in mission scheduling and security
716 inspections. This product is disseminated through TRACE and classified e-mail.
- 717 • **Modal Threat Assessments.** Modal Threat assessments, produced by analyst teams at
718 the classified level, provide more in-depth analysis and judgments on the threats posed to
719 the various transportation modes. They are disseminated through TRACE, NCTC
720 Online, and classified and unclassified e-mail.
- 721 • **No-Fly / Selectee Lists.** The No-Fly and Selectee Lists are subsets of the Terrorism
722 Screening Center's (TSC) master data base known as the Terrorism Screening Data Base
723 (TSDB). TSA does not own the lists, but does provide them to air carriers and enforces
724 their use to ensure that passengers are thoroughly prescreened before they are allowed to
725 enter the secure area of an airport or to board an aircraft. Individuals on the No-Fly list
726 pose or are suspected of posing threats to transportation or national security. The
727 Selectee list covers those individuals who do not meet the criteria for the No Fly List, but
728 who must receive additional screening prior to flying.
- 729 • **FAM Mission Briefs.** FAM Mission Briefs, country specific briefings produced at the
730 Secret Collateral level, cover terrorist and criminal threats, as well as other pertinent
731 information such as recent political unrest and health concerns within countries scheduled
732 for Federal Air Marshal mission coverage. The documents are disseminated via TRACE
733 and by classified facsimile to the 22 FAM field offices.
- 734 • **Homeland Intelligence Report (HIR).** The HIR is the Department of Homeland
735 Security's (DHS) reporting vehicle, used by DHS and its subordinate organizations, to
736 provide intelligence information to the IC and LE communities. HIRs do not contain
737 fully-evaluated intelligence. TSA produces HIRs to meet the standing information needs
738 of DHS and collection requirements of the greater intelligence community.
- 739 • **Spot Reports.** Spot Reports, a TSA-OI Watch product, share time-sensitive information
740 and provide situational awareness on persons who are denied boarding or in flight,
741 persons of interest to the LE or IC communities, or an event that has importance to TSA's
742 mission. Spot Reports can be both SBU and classified, if additional intelligence warrants
743 classifying the document. The reports are delivered to DHS for further distribution.
- 744 • **Collaborative Transportation Imagery Project (CTIP).** The CTIP develops
745 interactive imagery products of critical transportation infrastructure. These products
746 incorporate design schematics, interior and exterior photographs (360° immersive and
747 digital still), overhead imagery, digital video and essential emergency planning and
748 response documents. All imagery and documents are viewed through an interactive DVD
749 using hyperlinks and easy-to-navigate screens. The products can run on standard-issue
750 computers using off-the-shelf software.



Transportation Security Information Sharing Plan

Annual Update
October 2009

Transportation Security Administration



Homeland
Security

Foreword

I am pleased to present the following report regarding the Transportation Security Information Sharing Plan (TSISP). The report has been submitted pursuant to the *Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act)*, Pub. L. 110-53.

This annual report provides an update on the progress achieved from July 2008 to July 2009 in implementing the TSISP. The purpose of the TSISP is to establish a foundation for sharing transportation security information between all entities that have a stake in protecting the Nation's transportation system: Federal, State, local, and tribal (SLT) agencies and governments, the private sector, and foreign partners.

Pursuant to statutory requirements, this report is being provided to the Chairmen and Ranking Members of the House Transportation and Infrastructure Committee, the Senate Committee on Commerce, Science, and Transportation, the House Committee on Homeland Security, and the Senate Committee on Homeland Security and Governmental Affairs.

If I may be of further assistance, please do not hesitate to contact me or the TSA Office of Legislative Affairs, at (571) 227-2717.

Sincerely yours,

Gale D. Rossides
Acting Administrator

Executive Summary

The purpose of the TSISP is to establish a foundation for sharing transportation security information between all entities that have a stake in protecting the Nation's transportation system: Federal, State, local, and tribal (SLT) agencies and governments, the private sector, and foreign partners. Building on TSA's progress since its creation, implementing this plan further improves the way we share information and fight terrorism.

This plan considers the full range of information sharing among the public and private sectors. It encompasses cross-domain information sharing, which is the sharing of highly sensitive and classified intelligence information and the more general sharing of unclassified information that improves an entity's ability to prevent, protect, deter and recover from a terrorist attack. The plan addresses the current state of transportation information sharing and the future direction of systems and processes.

Congress provided funds to TSA in the Department of Homeland Security Appropriations Act, 2009, to further implement requirements associated with the *Implementing Requirements of the 9/11 Commission Act of 2007*. TSA identified its plan to establish and implement an Information Sharing and Analysis Center for transportation security in a required 9/11 Act Expenditure Plan (March 9, 2009). The Transportation Security Information Sharing and Analysis Center (TS-ISAC) will enable TSA to provide a continuous flow of information in a variety of formats to existing ISACs and other mission partners and enable virtual analytic collaboration. The implementation date is by spring 2010.

The five major functions of the TS-ISAC are:

- 1) **Dissemination.** TSA-OI will post finished intelligence products (unclassified), alerts, and downgraded intelligence reporting to our stakeholders on the ISAC Web portal.
- 2) **Alerts.** TSA-OI will send an e-mail message to the TS-ISAC user's e-mail account, indicating when an alert has been posted to the portal.
- 3) **Information Repository.** An information warehouse will serve as a repository of tacit and explicit transportation security knowledge to enable trend analysis and for future reference.
- 4) **Usability.** The TS-ISAC will be linked into the DHS Homeland Security Information Network (HSIN), where HSIN users will be able to click on a link and gain seamless (no log-on) entry into our portal.
- 5) **Collaboration.** The TS-ISAC will have the ability to conduct live video teleconferences with our stakeholders (live voice, video, and data).

This implementation plan focuses on the core capabilities needed to maximize information sharing across all communities of interest. As the security framework for transportation continues to grow, TSA and its Federal partners are working to apply many of these capabilities to reduce risk across all modes of transportation. The mission capabilities and the processes described in this plan will enhance current functions and will be leveraged across the transportation system.

Table of Contents

I.	Legislative Requirement	1
II.	Background	2
III.	TSA Information Sharing Analysis Center	6
IV.	Sharing Information at the Federal Level	10
V.	Appendices	16
	Appendix A: Abbreviations	
	Appendix B: Intelligence and Information Sharing Products	

I. Legislative Requirement

This document responds to the reporting requirement set forth in the *Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act)*, Pub. L. 110-53, Section 1203(a)(6)(B), which requires the submission of an annual report to the appropriate congressional committees on updates to and the implementation of the previously submitted (July 2008) Transportation Security Information Sharing Plan.

II. Background

Purpose

The *9/11 Commission Report*, released in July 2004, highlighted the importance of information sharing as a foundational element necessary in the fight against terrorism. Many of the recommendations documented in the *9/11 Commission Report* were mandated in the *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA).

On August 3, 2007, the President signed the *Implementing Recommendations of the 9/11 Commission Act of 2007* (9/11 Act), which includes measures associated with IRTPA and enhances existing information sharing endeavors. Section 1203 requires that the Secretary of Homeland Security establish a Transportation Security Information Sharing Plan (TSISP) in consultation with the Program Manager of the Information Sharing Environment (PM-ISE), the Secretary of Transportation, and public and private stakeholders¹.

The TSISP is closely aligned and consistent with the overarching National Strategy for Information Sharing, the Information Sharing Environment Implementation Plan (ISE-IP), the National Infrastructure Protection Plan (NIPP), and the Transportation Systems Sector Specific Plan (TS-SSP). It is also aligned with the DHS Information Sharing Strategy (dated May 12, 2008), which creates an essential link between the National Strategy, the ISE-IP, the TSISP, and with TSA's sector-specific plans.

The purpose of the TSISP is to establish a foundation for sharing transportation security information between all entities that have a stake in protecting the Nation's transportation system: Federal, State, local, and tribal (SLT) agencies and governments, the private sector, and foreign partners. Building on TSA's progress since its creation, implementing this plan further improves the way we share information and fight terrorism.

Goals

This plan considers the full range of information sharing among the public and private sectors. It encompasses cross-domain information sharing, which is the sharing of highly sensitive and classified intelligence information and the more general sharing of unclassified information that improves an entity's ability to prevent, protect, deter and recover from a terrorist attack. The plan addresses the current state of transportation information sharing and the future direction of systems and processes.

TSA solicited input and coordinated this plan with the Department of Transportation, the PM-ISE, and other public and private stakeholders. The plan was coordinated with the Transportation Sector Government Coordinating Council (GCC) and the mode-specific Sector Coordinating Councils (SCC). All comments and inputs were considered in the final version of this document. The GCC will propose to the SCC establishing a joint Information Sharing working group to implement this plan and improve future versions.

¹ "The term 'public and private stakeholders' means Federal, State, and local agencies, tribal governments, and appropriate private entities, including nonprofit employee labor organizations representing transportation employees." From *Implementing Recommendations of the 9/11 Commission Act of 2007*, Section 1203.

TSA will ensure that the plan and any future changes are reviewed through the DHS Information Sharing governance structure, and will continue to seek suggestions from all partners interested in information sharing for improving the information sharing process, which will be reflected in future updates to this plan.

The goals established in this plan are derived from the Information Sharing Environment Implementation Plan (ISE-IP) and focus on effectively sharing transportation security information in order to maintain the security of the Nation's transportation network. The goals are:

- **Multi-Directional Sharing:** Establish a framework enabling secure, multidirectional transportation security information sharing between government and industry.
- **Effective and Efficient Processes:** Establish clear governance, roles, responsibilities, and communication protocols between transportation security stakeholders to promote more rapid and effective exchange of information, analysis, and coordination.
- **Trusted Partnership:** Establish trusted partnerships among all levels of the transportation security network.
- **Right Information-Right People-Right Time:** Improve the timely and secure exchange of transportation security information supported by education, training, awareness programs, and enabling technologies.
- **Protect Privacy and Civil Liberties:** Ensure privacy and civil liberties are protected within the transportation security network.

The current information sharing process is designed to communicate both actionable information on threats and incidents as well as information pertaining to overall transportation sector status (e.g., plausible threats, vulnerabilities, potential consequences, incident situation, and recovery progress). This is accomplished through the collection, production, and sharing of information. It enables timely and effective decision-making so that owners and operators of critical infrastructure, SLT governments, and other security partners can assess risks, make appropriate security investments, and take effective and efficient protective actions.

Strategy

Since its creation DHS has sought innovative and effective ways to share information with all its stakeholders. Effective communications and information sharing is a pillar of DHS's strategic and operational approach. Effective communication is a difficult task given the complexity of the transportation security network and the vast number of stakeholders that span Federal and SLT government agencies, as well as private entities and foreign partners.

The Transportation System as a sector comprises all modes of transportation (i.e., aviation, maritime, mass transit, rail, highway, and pipeline) and is a vast, open, complex, and interdependent "networked" system that moves millions of passengers and goods. Disruptions in the transportation network can often have non-linear effects. As a result, what may initially appear as an isolated disturbance in the network can have a much greater impact within and beyond the sector.

In response, DHS's information sharing approach constitutes a shift from a hierarchical model to one reflecting the networked nature of the sector. It allows for distribution and access to information both vertically and horizontally; it also enables decentralized decision making and actions.

Within the Transportation Security Administration (TSA) each mode of transportation is organized under a single point of contact (POC) or a General Manager (GM) uniquely positioned for the sharing of transportation security information with public and private stakeholders. These GMs, many of whom are senior executives with significant experience in the sector for which they are responsible, chair their respective Government Coordinating Councils and are responsible for managing interactions with Federal, SLT, and private sector entities.

Structure

Intelligence and information sharing are at the core of the DHS transportation security strategy. Information sharing is a multi-directional activity that occurs informally through relationships and formally through communication policies, regulations, procedures, guidance, and tools.

DHS uses intelligence and analysis to prioritize security activities. Each day begins with briefings on the latest intelligence from the IC; that information drives the decision making process both operationally and strategically. In addition, DHS shares intelligence and information as appropriate with governmental partners and sector stakeholders for further dissemination to appropriate operating and security officials and front-line employees enabling them to make informed security decisions.

The primary mechanisms for the sharing of transportation security information and the coordination of intelligence activities can be categorized into four general areas:

Information Sharing Environment. IRTPA Section 1016 requires the Federal Government to create an ISE for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties. The ISE-IP defines the Federal Government's information sharing strategy and provides the building blocks needed to successfully implement an ISE.

In alignment with the PM-ISE, DHS is establishing its ISE, and has established a governance structure through the Information Sharing Governance Board (ISGB) and the Information Sharing Coordinating Council (ISCC), in which TSA full member. On June 22, 2009, DHS publicly released the Department of Homeland Security's Privacy and Civil Liberties Protection Policy, which implements the Privacy Guidelines established by the PM-ISE for sharing terrorism information. Additionally, TSA has taken steps to establish a transportation information sharing capability in alignment with the PM-ISE and DHS ISE, to provide the right information to the right people at the right time through collaboration within and across the transportation sector network.

Part of the transportation information sharing capability is providing homeland security and terrorism information to both regulated and unregulated stakeholders. For example, security programs are shared between TSA and appropriate regulated aviation stakeholders to develop, approve, and amend crucial Sensitive Security Information (SSI) documents. SSI is appropriately shared and protected within the Transportation ISE in accordance with Title 49 of the Code of Federal Regulations, part 1520 (49 CFR 1520).

Office of Intelligence. TSA is the Department lead on transportation-related intelligence and analysis. TSA's intelligence mission is to provide timely and accurate intelligence and information related to threats to transportation; this information is provided to TSA, DHS' Office of Intelligence and Analysis (I&A), DHS leadership and field entities, and other Federal and SLT authorities, as well as foreign partners. TSA functions as the operational conduit between the public and private transportation security stakeholders and the Intelligence Community (IC), and is a full partner with other DHS

intelligence components. TSA is a member component of the DHS Intelligence Enterprise, which is led and managed by the Department's Chief Intelligence Officer.

Sector Partnership Model. DHS uses the transportation sector partnership, specifically the GCC and mode-specific Sector Coordinating Council (SCC) structures, as the primary mechanism to coordinate transportation information sharing policy, strategy, plans, issues, and requirements development. Coordination with the DHS's information sharing coordinating bodies is ensured.

Transportation Security Operations Center (TSOC). The TSOC is a sophisticated 24-7 operations center that maintains continuous information sharing with Federal, SLT, and private transportation-related entities. It serves as the main POC for security-related incidents or crises in all modes of transportation and is the primary interface to the DHS National Operations Center (NOC) for these incidents or crises. The TSOC's mission is to coordinate and communicate intelligence and domain awareness information for U.S. transportation related security activities worldwide. Its strategic goals are incident prevention and/or interdiction, threat mitigation, and incident coordination and management.

III.TSA Information Sharing and Analysis Center

Description

Congress provided funds to TSA in the Department of Homeland Security Appropriations Act, 2009, to further implement requirements associated with the *Implementing Requirements of the 9/11 Commission Act of 2007*. TSA identified its plan to establish and implement an Information Sharing and Analysis Center for transportation security in a required 9/11 Act Expenditure Plan (March 9, 2009).

The Transportation Security Information Sharing and Analysis Center (TS-ISAC) will enable TSA to provide a continuous flow of information in a variety of formats to existing ISACs and other mission partners and enable virtual analytic collaboration. The implementation date is by spring 2010 (see Figure 1).

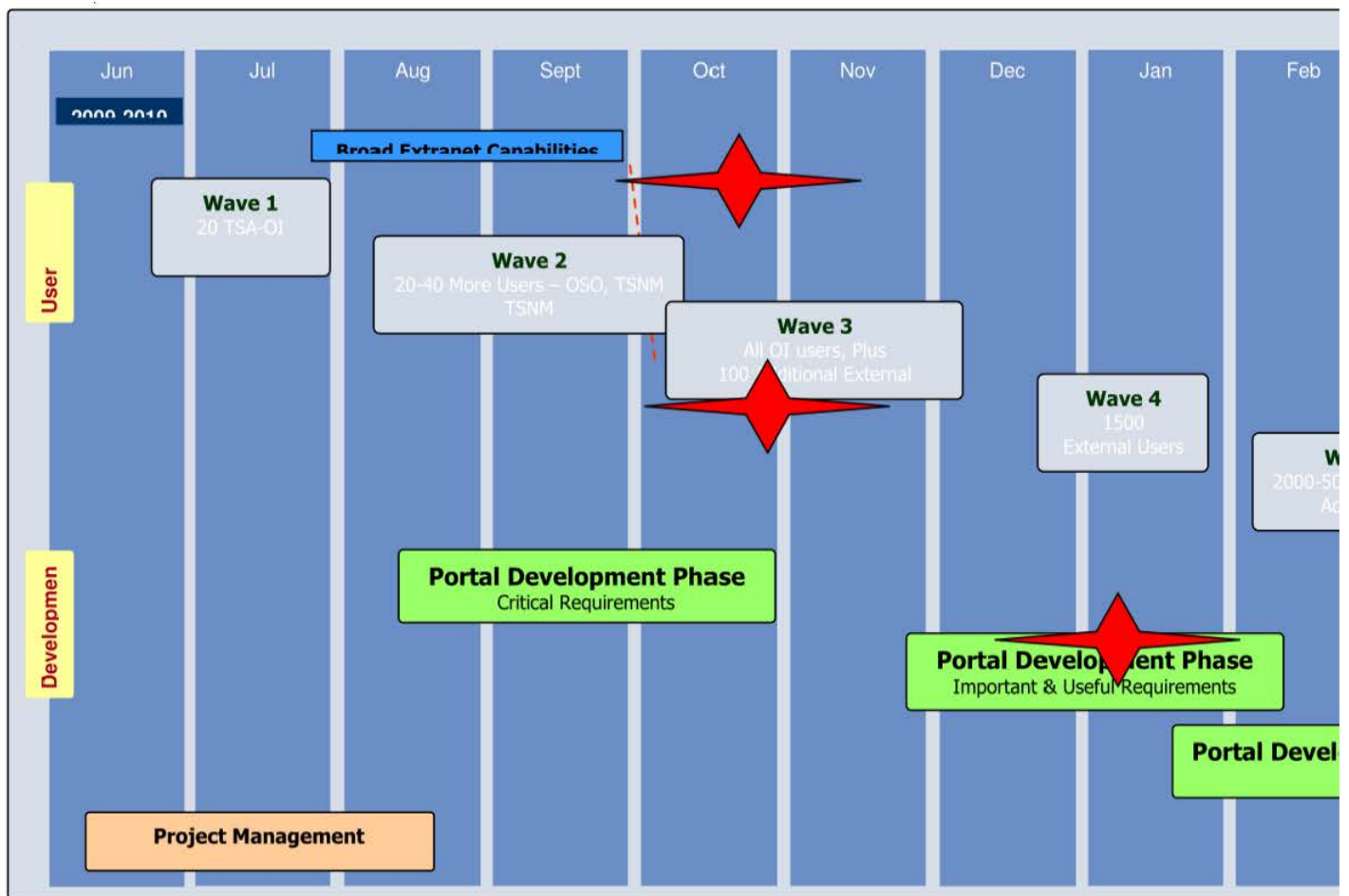


Figure 1: TS-ISAC Implementation Plan

The TS-ISAC provides an effective means to reach operating officials, law enforcement personnel, and security directors from all transportation modes.

TSA-OI will post all of our unclassified (FOUO) intelligence products to the TS-ISAC portal, as well as properly vetted documents from other transportation security partners and stakeholders (including media products).

The TS-ISAC is supported by information from the TSOC and TSA-OI's 24/7 Watch Center. Security awareness materials will continuously be provided during routine operations, as well as alerts and time-sensitive information during periods of heightened threat. When fully operational, the TS-ISAC will provide the capability for analysts to interact real-time through the use of audio and video virtual collaboration.

Transportation security information will be available for mission partners from a portal accessible via the Internet. It is anticipated that the TS-ISAC will be accessible from the TSA eShare site, a Web-based portal for those that do not have access to the TSA internal network, as well as from the DHS Homeland Security Information System (HSIN), since users are already approved by DHS to receive this information.

TSA-OI will replicate the TS-ISAC on the classified Homeland Security Defense Network (HSDN). The replication will be at a different classification level and will not interface with the unclassified TS-ISAC. The purpose is to share secret level information with state fusion centers, TSA Field Intelligence Officers, and other mission partners with access to HSDN, the Secret Internet Protocol Router Network (SIPRNET), and/or the TSA Remote Access to Classified Enclaves (TRACE) network.

The TS-ISAC will have a world-class design and appearance, with tools, functionality, reliability and security that is state-of-the-art. This unclassified Web-based portal will have sufficient DHS/TSA branding to clearly identify it as a government Website. Security will be provided via user ID and password plus the ability to utilize multi-factor authentication to comply with OMB 06-16 requirements for external users; TSA employees will not have to log on from a TSA internal system. This enables sharing of For Official Use Only (FOUO) intelligence products. Data will expire when TSA deems it necessary via use of a Data Loss Protection type of technology.

Functions

The five major functions of the of the TS-ISAC are:

Dissemination. TSA-OI will post finished intelligence products (unclassified), alerts, and downgraded intelligence reporting to our stakeholders on the ISAC Web portal. TSA-OI must review all finished products before publishing on the site; finished intelligence products will not be modifiable by users. The Web portal will be used to distribute information to the TSA workforce, Federal, state, local and tribal governments, and our private industry stakeholders.

Alerts. TSA-OI will send an e-mail message to the TS-ISAC user's e-mail account, indicating when an alert has been posted to the portal. The alert will be sent from the host to the users who have subscribed to receive an alert for a particular community of interest (e.g., aviation, mass transit, etc.). Alerts will also notify users of new product postings and contain a link to the site.

Information Repository. An information warehouse will reside within the TS-ISAC. This warehouse will serve as a repository of tacit and explicit transportation security knowledge to enable trend analysis and for future reference.

The TS-ISAC will reside in an IT-environment where the content access to intelligence information is controlled by the host (TSA-OI). This is particularly important for our ability to share “tearline” information with our stakeholders. Tearline intelligence information is sanitized to make it available at a lower classification level. TSA must ask the originator of the information for permission to share the downgraded intelligence with a specific group of people – therefore, we need to approve users who are able to view certain specific information that we post. TSA-OI will determine what information is provided and/or available to the users, including tearlines of intelligence information. The users will be able to comment on this type of information, but such content will not be able to be modified.

Additionally, The TS-ISAC is the primary means for all of our stakeholders (industry and government) to access and utilize our TSA Risk Management Tools. Some of these tools may be maintained on a TSA server that will interface directly with the TS-ISAC. Other risk-based tools will be Web-based applications and documents. The tools will be modifiable by TSA personnel only, but the modeling functions will be accessible for some of our stakeholders to utilize; users must have special access rights to use some of the risk tools.

Usability. The TS-ISAC will be linked into the DHS Homeland Security Information Network (HSIN), where HSIN users will be able to click on a link and gain seamless (no log-on) entry into our portal. This will alleviate the need for much of the vetting for users of the system.

According to DHS Management Directive 11042.1 (Safeguarding Sensitive but Unclassified Information), access to FOUO information is based on a “need to know” as determined by the holder of the information—therefore the information is approved to be provided on the TS-ISAC.

Collaboration. The portal will contain tools to foster information sharing within the transportation security community as noted above. In the future, the TS-ISAC will have the ability to conduct live video teleconferences with our stakeholders (live voice, video, and data). Additionally, TS-ISAC users will be able to “collaborate” in the same manner with each other as they are able to with DHS on the HSIN.

The TS-ISAC will have the following collaborative functionality for the systems users:

- Facebook or MySpace type of area for users to populate information about themselves
- Provide feedback on finished intelligence
- Submit requests for information
- Enter real-time blog and Web forum entries
- Participate in chat rooms with other users
- Submit products to TSA-OI for inclusion in the finished documents section
- Recommend edits to draft products
- Submit questions/input while attending virtual meetings
- View documents and videos which are posted to the site
- Print documents

- Sign-up to receive alert messages sent from the host
- Access the communities of interest
- Perform key word searches on information within the portal
- Utilize TSA risk tools
- Access the portal from DHS HSIN
- Access the portal from TSA iShare with no need to log-on a second time

The following are functions that will **not** be available for the TS-ISAC portal users:

- Anonymous posting of information
- Modification of finished documents posted to the site
- Ability to access the site and collaborative tools without user access
- Modification of the TS-ISAC portal/pages design
- Posting of documents directly to the portal, or deleting documents from the portal
- Wikis or Wikipedia-like entries (only for select groups in a private location)
- Ability to access information outside of what is provided on the site

Access to the portal must be limited to properly vetted individuals only. Additionally, the portal will be segregated into communities of interest based on modes of transportation. All users will have access to all the different communities of interest, enhancing the ability to share information across different modes.

IV. Sharing Information at the Federal Level

Processes

DHS shares transportation security information with other Federal Government partners through the organizational constructs delineated in this plan. This includes, but is not limited to, the ISE, the Interagency Threat Assessment and Coordination Group, and the NIPP and corresponding TS-SSP.

Additionally, as Federal partners develop information sharing strategies specific to their mission and operational goals, DHS will collaborate with these groups to leverage existing information sharing plans, minimize duplicative documentation, and maximize returns from information sharing investments. This collaborative approach at the Federal level will in turn drive the manner in which terrorism-related information is shared with non-Federal partners.

Within DHS, TSA serves as the primary transportation security liaison to the intelligence and law enforcement communities. TSA's intelligence mission is to provide timely and accurate intelligence and information related to threats to transportation to TSA and DHS leadership, field entities, and other Federal and SLT authorities (see Figure 2). In support of TSA's mission, the TSOC integrates information provided by TSA-IO, fusing actionable intelligence with operational information across all modes of transportation.

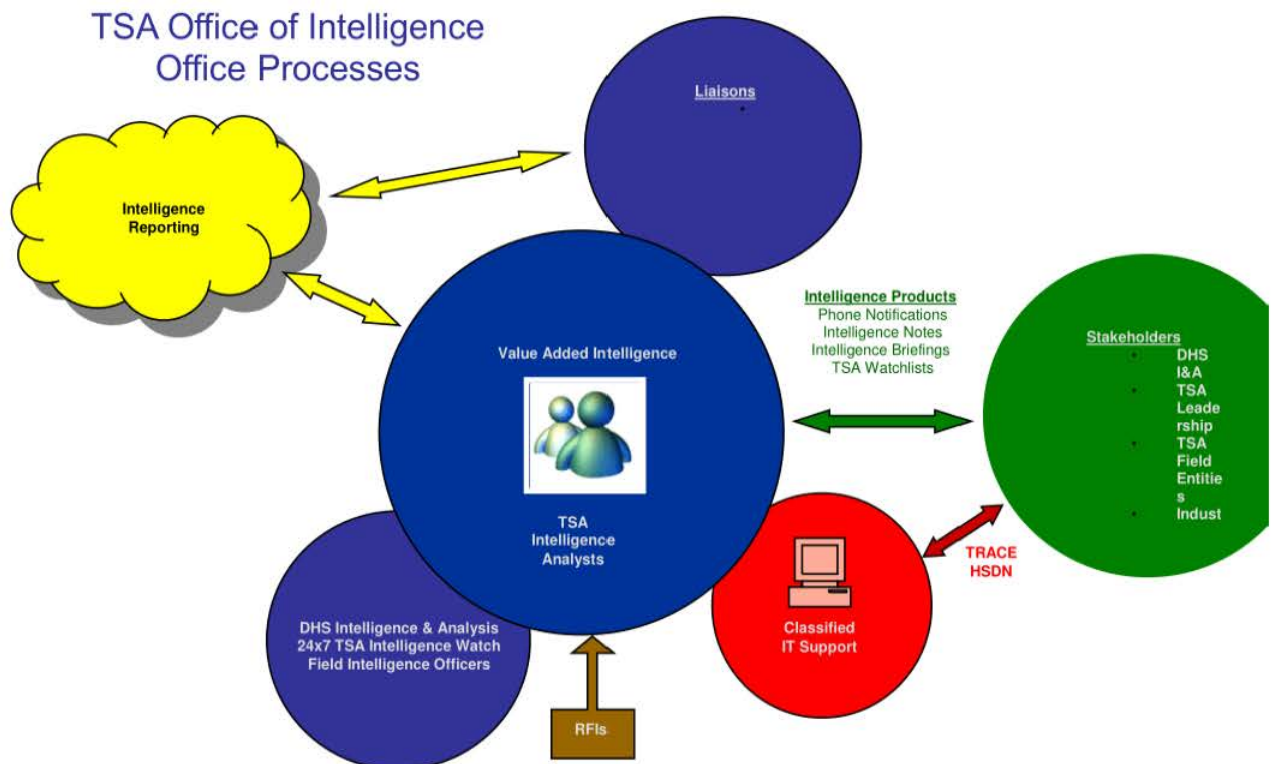


Figure 2: Intelligence Reporting Process

Technologies

DHS uses technologies, consistent with the ISE, to communicate cross-domain (i.e., classified and unclassified) information with its Federal partners, including:

- **Joint Worldwide Intelligence Communications System (JWICS):** A system of interconnected computer networks used to transmit classified information in a secure environment.
- **INTELINK:** A highly secure intranet used by the U.S. IC. It serves as the Web environment on protected top secret, secret, and unclassified networks.
- **Homeland Secure Data Network (HSDN):** Functioning as DHS's secure communications infrastructure, it allows Federal and SLT governments to share timely and actionable classified information. It is a major secure information thoroughfare joining together intelligence agencies, law enforcement, disaster management, and front-line disaster response organizations in the common goal of protecting our Nation and its citizens.
- **Secret Internet Protocol Router Network (SIPRNet):** A system of interconnected computer networks used to transmit classified information in a secure environment.
- **Non-secure Internet Protocol Router Network (NIPRNet):** Used to exchange sensitive but unclassified information between internal users as well as providing user access to the Internet.
- **TSA Remote Access to Classified Enclaves (TRACE):** A high-speed, National Security Agency-approved system designed to quickly and securely provide remote TSA field locations with classified and unclassified intelligence information. Currently this system supports up to the Secret Collateral security level.
- **TSA Automated Inspections, Enforcement, and Incident Reporting Subsystem.** This system supports a broad range of mission requirements including data capture of critical records documenting security compliance and oversight inspections; outreach contacts with industry stakeholders; administrative enforcement and regulatory investigations; and the details and the subjects associated with reported security incidents. This enterprise application serves more than 5,000 authorized internal users. Data outputs support external Freedom of Information Act requests, internal operations research, and out-of-agency requests for transportation security statistics. Currently housing more than a million individual subject name records, this application also augments the critical functions performed by several organizational elements; namely the Office of Intelligence, the Sector Partnership Model, and TSA's 24/7 operations center. Planned strategic expansion will accommodate a growing enterprise and facilitate the swift exchange of data and analysis.

TSA also provides information through a variety of intelligence products, which are delineated in Appendix B to this plan.

SLT Integration

Other Federal, State, local, and tribal (SLT) agencies and governments are critical to our Nation's efforts to prevent future terrorist attacks and are the first to respond if an attack occurs. These entities carry out their counterterrorism responsibilities within the broader context of their core mission to protect the public's health and safety and to provide emergency and non-emergency services.

DHS has an integrated approach that allows Federal agencies to work together to produce and disseminate terrorism information. This includes:

- **Fusion Centers:** These centers integrate relevant law enforcement and intelligence information analysis and coordinate security measures to reduce threats in their communities. Fusion centers serve as focal points for the receipt and sharing of terrorism-related information, and play a vital role in disseminating terrorist information at the state level. DHS supports these centers through grant funding, technical assistance, and training; and by deploying departmental officers and intelligence analysts to fusion centers nationwide to achieve a baseline level of capability.
- **Joint Terrorism Task Forces (JTTF):** DHS has a significant presence in JTTFs in major cities throughout the United States. TSA's Federal Air Marshal Service has representatives on all 56 major Federal Bureau of Investigations Field Office JTTFs and several of its resident office JTTFs. These task forces have substantially contributed to improved information sharing and operational capabilities at the State and municipal levels.
- **National Infrastructure Coordination Center (NICC):** Serves as an extension of the NOC, providing the mission and capabilities to assess the operational status of the Nation's Critical Infrastructures and Key Resources, supports information sharing with the ISACs and the owners and operators of critical infrastructure facilities, and facilitates information sharing across and between the individual sectors.

Private Sector Integration

Private industry within the transportation sector has made significant investments in mechanisms and methodologies to evaluate, assess, and exchange information across regional, market and security-related communities of interest (COIs). DHS continues to build an effective framework that ensures a two-way flow of timely and actionable security information between public and private partners.

DHS has established several information sharing mechanisms to disseminate and receive information with the private sector. These include:

- **Critical Infrastructure Partnership Advisory Council (CIPAC):** CIPAC provides a legal framework for members of the GCC and SCC to collaborate on a broad spectrum of security activities. This approach aligns with the NIPP, the corresponding TS-SSP, the ISE-IP, and other information sharing guidance. The SCC plays an important role in providing the private sector perspective on identifying and implementing the information sharing mechanisms that are most appropriate for their modes of transportation.
- **Homeland Security Information Network:** DHS communicates in real-time to its partners by utilizing the internet-based HSIN. System users include governors, mayors, Homeland Security Advisors, State National Guard offices, emergency operations centers, first responders, public safety departments, and other key homeland security partners. HSIN is a highly secure network

with a common set of information-sharing functions and tools for various private sector communities with common security interests. It is sponsored by DHS and managed by the private sector-led SCC and/or its designees. The mode specific sub-portals are currently in various stages of development, with three modes of transportation – Mass Transit, Highway and Motor Carrier, and Pipeline– with fully functioning portals.

- **Homeland Infrastructure Threat and Risk Analysis Center (HITRAC):** HITRAC is the national infrastructure integration center for threat and risk. This office, jointly resourced by the DHS Office of Infrastructure Protection and DHS I&A, provides primary, collaborative, and integrative tactical and strategic intelligence and assessments of threats to the Nation's critical infrastructure. HITRAC develops intelligence products to help inform State and Local Fusion Centers and infrastructure owners and operators of any threats they may potentially face, as well as to better inform their security planning and investment decisions. HITRAC collaborates with TSA for intelligence assessments and uses transportation threat and risk assessments to inform assessments of other sectors based on dependencies on transportation. HITRAC provides the threat assessments for annual grants and responses to the state and Urban Areas Security Initiative city assessments.
- **Information Sharing and Analysis Centers:** ISACs play a vital role in facilitating communication and coordination of information related to terrorism. DHS works with transportation industry ISACs on a daily basis to address security issues. Various ISACs have access to and work with the TSOC, and with TSA's modal experts and intelligence personnel. ISAC personnel have access to information and intelligence consistent with security policies.
- **Sensitive Security Information (SSI):** This statutory and regulatory-based framework for transportation security-related Sensitive but Unclassified information allows streamlined and safe sharing with SLT governments, law enforcement, and private industry to enhance transportation security.
- **Protected Critical Infrastructure Information Program (PCII):** This statutory and regulatory-based framework enables the private sector to voluntarily submit sensitive information regarding the Nation's critical infrastructure to DHS with the assurance that the information, if it meets certain requirements, will be protected from public disclosure. The program seeks to facilitate greater sharing of critical infrastructure information among owners and operators and government entities with infrastructure protection responsibilities, thereby reducing the Nation's vulnerability to terrorism.

To better partner with SLT governments, and the private sector, DHS deploys a cadre of highly-experienced security specialists in regions throughout the country to assist local efforts to protect critical assets and provide a local perspective to the national risk picture. With significant experience in emergency management, these DHS Protective Security Advisors (PSAs) are dedicated critical infrastructure and vulnerability assessment experts who are recruited from, live, and work in these communities. They provide a federally funded resource to communities and businesses to assist in the protection of critical assets.

International Cooperation

The sharing of terrorism-related information between Federal departments and agencies and foreign partners and allies is a critical component of our information sharing strategy. After the September 11 attacks, many foreign governments joined us in declaring war on terrorism and have since contributed in important ways. Intelligence provided by foreign partners often provides the first indications of terrorist plans and intentions.

It is critical that we appropriately share similar types of information with foreign governments or foreign law enforcement entities such as INTERPOL. We must ensure that any sharing of any records about American citizens and lawful permanent residents is in compliance with U.S. privacy rights and protections.

The mission of TSA's Office of Global Strategies is to increase security by working proactively with foreign partners and overseas operations that affect the United States. TSA has significantly strengthened our relationships with international transportation security partners through increased communications, information sharing, and best practices. Examples of international cooperation that the Office of Global Strategies will increase and strengthen include common strategies on screening liquids, aerosols, and gels, and implementing advanced technologies and intelligence sharing.

Other activities include:

- **European Union Passenger Name Record Agreement:** The United States and the European Union have agreed to a security program that shares personal data about millions of United States-bound airline passengers a year. Under the agreement, airlines flying from Europe to the United States are required to provide data related to these matters to U.S. authorities if it exists in their reservation systems. The agreement allows DHS to retain and use it "where the life of a data subject or of others could be imperiled or seriously impaired," such as in a counterterrorism investigation.
- **Transportation Security Administration Representatives (TSARs):** These personnel serve as official TSA representatives around the world. TSARs are located in foreign countries and work closely to share information with their governments to improve international transportation security. TSA also has an experienced corps of aviation security experts based internationally with regulatory and inspection responsibility that also share information. Their talents can meaningfully increase security measures in cooperation with airlines and other governments.

Conclusions

The TSISP requires a multiple-phase implementation over several fiscal years, with initial activities focused on the expansion of mission capabilities within DHS and the foundational components necessary to expand mission services to other Federal agencies. Subsequent phases will deploy mission capabilities, based on stakeholder prioritization, to other Federal and SLT authorities, private sector stakeholders, and foreign partners in addition to the continuation of advancements in DHS workspaces.

This implementation plan focuses on the core capabilities needed to maximize information sharing across all communities of interest. As the security framework for transportation continues to grow, TSA and its Federal partners are working to apply many of these capabilities to reduce risk across all modes of transportation. The mission capabilities and the processes described in this plan will enhance current

functions and will be leveraged across the transportation system. In addition, as our information sharing efforts mature, policy and technology will lead to the introduction of additional information sources not currently included or available with these communities.

Appendix (A)

List of Acronyms

The following acronyms are used in this document:

9/11 Act	Implementing Recommendations of the 9/11 Commission Act of 2007
ADIB	Administrator's Daily Intelligence Briefing
CATA	Cities & Airports Threat Assessment
CIPAC	DHS Critical Infrastructure Partnership Advisory Council
COI	Communities of Interest
CTIP	Collaborative Transportation Imagery Project
DHS	Department of Homeland Security
DHS I&A	DHS Office of Intelligence and Analysis
FIO	Field Intelligence Officers
GCC	Transportation Sector Government Coordinating Council
GM	General Manager
GFE	Government Furnished Equipment
HIR	Homeland Intelligence Report
HITRAC	Homeland Infrastructure Threat and Risk Analysis Center
HSDN	Homeland Secure Data Network
HSIN	Homeland Security Information Network
IC	Intelligence Community
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
ISAC	Information Sharing and Analysis Center
ISCC	Information Sharing Coordination Councils
ISE	Information Sharing Environment
ISE-IP	Information Sharing Environment Implementation Plan
JTTF	Joint Terrorism Task Forces
JWICS	Joint Worldwide Intelligence Communications System
NCTC	National Counterterrorism Center
NICC	National Infrastructure Coordination Center
NIPP	National Infrastructure Protection Plan
NIPRNet	Unclassified but Sensitive Internet Protocol Router Network
NOC	DHS National Operations Center
PCII	Protected Critical Infrastructure Information Program
PM-ISE	Program Manager of the Information Sharing Environment
POC	Point Of Contact
PSA	Protective Security Advisors
SBU	Sensitive But Unclassified
SCC	Mode-specific Sector Coordinating Councils
SIPRNet	Secret Internet Protocol Router Network
SIR	Suspicious Incidents Report
SLFC	State and Local Fusion Centers
SLPMO	State and Local Program Management Office
SLT	State, Local, and Tribal
SSI	Sensitive Security Information
TFS	Two-Factor Authentication
TIG	Transportation Intelligence Gazette
TRACE	TSA Remote Access to Classified Enclaves
TSA	Transportation Security Administration
TSA-OI	TSA Office of Intelligence

TSAR	Transportation Security Administration Representatives
TS-ISCC	Transportation Security Information Sharing Coordination Council
TS-ISAC	Transportation Security Information Sharing and Analysis Center
TSISP	Transportation Security Information Sharing Plan
TSOC	Transportation Security Operations Center
TS-SSP	Transportation Systems Sector Specific Plan
WFIS	Weekly Field Intelligence Summary

Appendix (B)

Intelligence and Information Sharing Products

The TSA Office of Intelligence (TSA-OI) operates a 24-7 indications and warnings watch. The Watch is connected to the IC and DHS I&A via JWICS, HSDN and SIPRNET, which provide the watch with access to both intelligence reporting from the field and finished intelligence products, including assessments. The headquarters watch has real-time access and contact with all U.S. IC watches and operations centers. This access allows TSA-OI to receive and provide real and near real-time intelligence on threats to the U.S. transportation system.

TSA-OI provides detailed value added analytical products, in the form of classified and unclassified briefings, assessments, and summaries. These products are presented to TSA/DHS leadership, SLT authorities and law enforcement, TSA field entities and representatives, foreign officials and private sector stakeholders. Under the 49 CFR 1500 series, TSA may issue an Information Circular to notify stakeholders about security concerns. When TSA determines the additional security measures are necessary to respond to a threat assessment or to a specific threat against civil aviation, TSA issues a Security Directive setting forth mandatory measures.

TSA-OI also has Field Intelligence Officers (FIOs) at airports around the United States. The FIOs interact with TSA officials, other Federal agencies and SLT officials in areas to which they are assigned. They are the face of TSA-OI for all intelligence support and activities outside of the Washington D.C. area.

TSA provides the following intelligence and information sharing products to partners and stakeholders on a routine basis:

- **Administrator's Daily Intelligence Briefing (ADIB).** A 24-hour snapshot of transportation-related intelligence comprised of TSA operational and Intelligence Community reporting. This product is disseminated through TRACE and classified e-mail to a limited TSA audience.
- **Transportation Intelligence Gazette (TIG).** The TIG, usually a classified analytic document, aims to bridge the gap between the ADIB and modal threat assessments by providing in-depth analysis focused on a specific topic within a transportation mode. The document may also be used to provide additional information or background on an issue, or to provide situational awareness. TIG lengths vary and are disseminated through TRACE, NCTC Online, HSIN Intel, HSDN, and classified and unclassified email lists.
- **Suspicious Incidents Report (SIR).** The SIR provides a weekly summary and analysis of operational reporting on suspicious activities and surveillance directed against all transportation modes. Sources for the SIR include law enforcement (LE) and IC reporting. This product is available in both classified and SSI editions and is disseminated via multiple LE and IC distributions lists, portals, and Web boards.
- **Weekly Field Intelligence Summary (WFIS).** The WFIS is a weekly analytical summary of law enforcement and open source reporting produced at the SSI level. The document provides information on threats, significant airport and aircraft incidents, and IC and LE advisories. The WFIS is disseminated via a Sensitive Security Information (SSI) distribution list and posted on LE and IC portals and Web boards.
- **Cities & Airports Threat Assessment (CATA).** The CATA is a classified and SSI-level domestic and overseas flight risk assessment provided to TSA International, Federal Air Marshals, and Airport Security Inspectors to assist in mission scheduling and security inspections. This product is disseminated through TRACE and classified e-mail.

- **Modal Threat Assessments.** Modal Threat assessments, produced by analyst teams at the classified level, provide more in-depth analysis and judgments on the threats posed to the various transportation modes. They are disseminated through TRACE, NCTC Online, and classified and unclassified e-mail.
- **No-Fly / Selectee Lists.** The No-Fly and Selectee Lists are subsets of the Terrorism Screening Center's (TSC) master data base known as the Terrorism Screening Data Base (TSDB). TSA provides the lists to air carriers and enforces their use to ensure that passengers are thoroughly prescreened before they are allowed to enter the secure area of an airport or to board an aircraft. Individuals on the No-Fly list pose or are suspected of posing threats to transportation or national security. The Selectee list covers those individuals who do not meet the criteria for the No Fly List, but who must receive additional screening prior to flying.
- **FAM Mission Briefs.** FAM Mission Briefs, country specific briefings produced at the Secret Collateral level, cover terrorist and criminal threats, as well as other pertinent information such as recent political unrest and health concerns within countries scheduled for Federal Air Marshal mission coverage. The documents are disseminated via TRACE and by classified facsimile to the 22 FAM field offices.
- **Homeland Intelligence Report (HIR).** The HIR is the Department of Homeland Security's (DHS) reporting vehicle, used by DHS and its subordinate organizations, to provide intelligence information to the IC and LE communities. HIRs do not contain fully-evaluated intelligence. TSA produces HIRs to meet the standing information needs of DHS and collection requirements of the greater intelligence community.
- **Spot Reports.** Spot Reports, a TSA-OI Watch product, share time-sensitive information and provide situational awareness on persons who are denied boarding or in flight, persons of interest to the LE or IC communities, or an event that has importance to TSA's mission. Spot Reports can be both SBU and classified, if additional intelligence warrants classifying the document. The reports are delivered to DHS for further distribution.



The Transportation Security Administration

Report to Congress

The Voluntary Provision of Emergency Services Program

December 2008

Executive Summary

The Voluntary Provision of Emergency Services Program (VPESP) allows “qualified individuals,” defined as law enforcement officers, firefighters and emergency medical technicians, to volunteer to assist with in-flight emergencies on commercial aircraft. Section 563 of the Senate-passed version of H.R. 2638, the Fiscal Year (FY) 2008 Department of Homeland Security (DHS) Appropriations Bill, proposed to require the Transportation Security Administration (TSA) to conduct a study on the implementation of VPESP and to report its findings to Congress. The Explanatory Statement that accompanies the FY 2008 DHS Appropriations Act (P.L. 110-161) directs TSA to comply with the terms and conditions listed in Section 563 of the Senate-passed bill. This report chronicles TSA’s study and findings, and lists action items derived from those findings.

TSA believes that VPESP gives aircraft passengers an additional level of safety by allowing qualified individuals to use their expertise to help flight crews in an emergency. The program augments emergency procedures already established by aircraft operators and offers crewmembers additional options during an in-flight emergency. VPESP is currently required of domestic aircraft operators that adopt a full security program in accordance with federal regulations.

Introduction

The Explanatory Statement directs TSA to conduct a study on the implementation of the VPESP established by 49 U.S.C. 44944(a), and to submit to Congress a report on its findings. Specifically, the Senate language states:

(a) Study on Implementation of Voluntary Provision of Emergency Services Program—

(1) Not later than 180 days after the date of enactment of this Act, the Administrator of the Transportation Security Administration shall conduct a study on the implementation of the voluntary provision of emergency services program established pursuant to section 44944(a) of title 49, United States Code (referred to in this section as ‘the program’).

(2) As part of the study required by paragraph (1), the Administrator shall assess the following:

(A) Whether training protocols established by air carriers and foreign air carriers include training pertinent to the program and whether such training is effective for the purposes of the program.

(B) Whether employees of air carriers and foreign air carriers responsible for implementing the program are familiar with the provisions of the program.

(C) The degree to which the program has been implemented in airports.

(D) Whether a helpline or other similar mechanism of assistance provided by an air carrier, foreign air carrier, or the Transportation Security Administration should be established to provide assistance to employees of air carriers and foreign air carriers who are uncertain of the procedures of the program.

(3) In making the assessment required by paragraph (2)(C), the Administrator may make use of unannounced interviews or other reasonable and effective methods to test employees of air carriers and foreign air carriers responsible for registering law enforcement officers, firefighters, and emergency medical technicians as part of the program.

(4)(A) Not later than 60 days after the completion of the study required by paragraph (1), the Administrator shall submit to Congress a report on the findings of such study.

(B) The Administrator shall make such report available to the public by Internet web site or other appropriate method.

This report is submitted to Congress in response to this requirement.

Background

After the September 11, 2001, terrorist attacks, Congress passed the Aviation and Transportation Security Act (ATSA) of 2001 (P.L. 107-71). Section 131(a) of ATSA enacted 49 U.S.C. 44944, which requires TSA to develop a program allowing “qualified individuals,” defined as law enforcement officers, firefighters and emergency medical technicians, to volunteer on commercial flights to assist with in-flight emergencies on commercial aircraft. This program is known as the Voluntary Provision of Emergency Services Program or “VPESP.”

In addition, under 49 U.S.C. 44944(b) and (c), qualified individuals who provide or attempt to provide assistance during an in-flight emergency will be eligible for an exemption from liability unless they render assistance in a manner that constitutes gross negligence or willful misconduct.

To participate in VPESP, qualified individuals must volunteer at the time of check-in and present the necessary credentials. Volunteering can only be done at check-in because appropriate credentials are required for acceptance into the VPESP. Once the credentials are validated, the aircraft operator is responsible for ensuring that crewmembers are aware of the identities, professions and seat locations of any VPESP volunteers on their flights. Given the operational differences among air carriers, the VPESP allows aircraft operators to determine the best way to comply with this requirement.

Since July 10, 2006, TSA has required a VPESP for any domestic aircraft operator that adopts a full security program in accordance with 49 CFR 1544.101(a). This security program, known as the Aircraft Operator Standard Security Program (AOSSP), is required for any scheduled passenger or public charter flight operation on aircraft with a seating configuration of 61 or more seats that enplane from or deplane into an airport sterile area. Currently, 66 domestic aircraft operators must comply with the AOSSP for all or part of their operations.

TSA has issued a Notice of Proposed Rulemaking (NPRM) that proposes, in part, to codify the VPESP and the exemption from liability into the Code of Federal Regulations.¹

Study Results/Analysis

This study was based on a review of the VPESPs of the 66 domestic aircraft operators that have adopted an AOSSP for all or part of their operations. VPESPs of foreign air carriers were not included in the study. TSA conducted this study using a survey that investigated the four subject areas outlined in Section 563(a)(2)(A)-(D) of the Senate-passed version of H.R. 2638. Each is addressed in turn:

Section 563(a)(2)(A) & (B): Whether training protocols established by air carriers and foreign air carriers include training pertinent to the program and whether such training is effective for the purposes of the program and whether employees of air carriers and foreign air carriers responsible for implementing the program are familiar with the provisions of the program.

TSA does not currently require aircraft operators to provide employees VPESP training. However, more than three-quarters of aircraft operators surveyed have developed and initiated VPESP training. An additional percentage of aircraft operators are committed to developing this type of training. Table 1 below outlines the number of aircraft operators that conduct or plan to conduct VPESP training. Table 2 below outlines how aircraft operators conduct VPESP training.

Table 1: Aircraft Operators that Provide VPESP Training to their Employees

Does the Aircraft Operator Provide Training to Employees Responsible for VPESP?		
<i>Yes: 52 (79%)</i> <i>(See Tables 2 & 3)</i>	<i>Under Development: 4 (6%)</i> <i>(See Table 4)</i>	<i>No: 10 (15%)</i> <i>(See Table 5)</i>

Table 2: How Aircraft Operators Conduct VPESP Training

How do the 52 (79%) Aircraft Operators Provide Training to VPESP?					
Classroom		Online		Training Bulletin/Manual	
<i>Once: 13²</i> <i>(25%)</i>	<i>Recurrent³: 5</i> <i>(10%)</i>	<i>Once: 8</i> <i>(15%)</i>	<i>Recurrent: 5</i> <i>(10%)</i>	<i>Once: 21</i> <i>(40%)</i>	<i>Recurrent: 0</i> <i>(0%)</i>

¹ Large Aircraft Security Program NPRM, 73 FR 64790 (October 30, 2008).

² Two of the carriers contained in this data conduct initial training in a classroom and annual recurrent training online after that.

³ "Recurrent" refers to training conducted on an annual cycle.

The survey collected information on how many of the aircraft operators that provide VPESP training require a demonstration of employee proficiency or understanding of VPESP requirements. The study yielded a variety of responses which are outlined in Table 3 below.

Table 3: Demonstrating Proficiency to VPESP

Do the 52 (79%) Aircraft Operators Require Trainees to Demonstrate Proficiency?	
YES: 12	NO: 40
How?	Why not?
# that conduct testing: 3	# that deem training adequate: 9
# that track VPESP enrollments and provide remedial training to staff if necessary: 3	# that did not provide an answer: 7
# that believe successful completion of training demonstrates proficiency: 3	# that always keep procedures available to employees (intranet, helpdesk and/or manuals): 6
# that conduct daily tracking of VPESP: 1	# that claim employees are subject to random testing: 2
# that believe annual training reinforces proficiency: 1	# that have employees sign training bulletins to demonstrate they are aware of the procedures: 15
# that conduct a roundtable upon training completion: 1	# that expect their employees to know VPESP as part of their job: 1

Twenty-one percent of aircraft operators surveyed answered that VPESP training is under development or they do not provide VPESP training to their employees. Table 4 below provides additional information on the four aircraft operators that are developing training. Table 5 below provides additional background from the 10 aircraft operators who have declined to provide VPESP training.

Table 4: VPESP Training is Under Development

Of the 4 (6%) Aircraft Operators Whose Training is Under Development
that simply stated training is under development: 2
that were confused with the requirements but will add VPESP training to their curriculum: 1
that began training its employees to VPESP during the study: 1

Table 5: Do not Provide VPESP Training

Of the 10 (15%) Aircraft Operators Who do not Provide Training:
that claimed their current emergency procedures were already in compliance with VPESP: 4
that believed this program was impractical to implement when very few people volunteer: 1
that stated they would be willing to train to VPESP. If they had a better understanding of it: 1
that admitted they were not aware of the program: 1
that believed the program had not been implemented: 1
that stated their contracting carrier provides the training: 2

In summary, notwithstanding that there is no specific training requirement in the VPESP, TSA expects aircraft operators to implement VPESP and ensure that employees responsible for implementing the procedures are fully aware of the provisions of the program, in accordance with AOSSP Section 6.15. The study shows that the majority of aircraft operators have provided VPESP training to these employees using methods such as training bulletins, classroom training or online training modules.

However, our study also revealed some aircraft operators have not implemented the VPESP program for various reasons. Some have asserted that current in-flight emergency procedures provide crewmembers with the option to seek out voluntary emergency service personnel and would meet the requirements of VPESP. The remaining aircraft operators claimed they either were not aware of VPESP, did not understand it, or believed that the VPESP was impractical to implement. TSA Principal Security Inspectors (PSIs) continue to provide assistance and counseling to Aircraft Operator Security Coordinators (AOSC) to facilitate compliance with the VPESP.

Section 563(a)(2)(C): The degree to which the program has been implemented in airports.

Eighty percent of aircraft operators surveyed reported that VPESP is implemented at all domestic locations served by their airline. Table 7 below provides additional information or justifications for why VPESP is not implemented at all locations served by the aircraft operator.

Table 6: VPESP Implementation at Airports

Is the Program Implemented at all Domestic Airports Served by the Aircraft Operator?	
YES: 53 (80%)	No: 13 (20%)

Table 7: Do not Implement VPESP at Domestic Airports

Of the 13 (20%) Carriers that do not Implement VPESP at Domestic Airports:
that claimed it's difficult when they primarily conduct charter operations: 6
that would implement once part of training: 2
that claimed it was unnecessary since onboard emergency procedures already in compliance: 1
that stated it is impractical to implement program of which volunteers are unaware: 1
that admitted they do not understand the program: 1
that implemented the program only at airports where they operate under an AOSSP: 1
that admitted they are not aware of the program: 1

As part of the AOSSP, aircraft operators are required to implement VPESP at any domestic location they serve. To date, 80 percent of aircraft operators have met this requirement. Of the remaining aircraft operators that operate under a Private Charter Standard Security Program (PCSSP), six primarily conduct private charter operations from non-federalized airports under the Private Charter program for which they are required to carry out VPESP. Nevertheless, four of these six aircraft operators have trained cabin crewmembers in VPESP to prepare for a qualified individual to volunteer emergency services before boarding an aircraft.

Of the aircraft operators that do not have the program at domestic stations, some believe current in-flight emergency procedures meet the requirements of VPESP, some are developing training, and some indicate a lack of knowledge of the program. TSA PSIs continue to provide assistance and counseling to Aircraft Operator Security Coordinators (AOSC) to facilitate compliance with the VPESP.

Section 563(a)(2)(D): Whether a helpline or other similar mechanism of assistance provided by an air carrier, foreign air carrier, or the Transportation Security

Administration should be established to provide assistance to employees of air carriers and foreign air carriers who are uncertain of the procedures of the program.

Only 29 percent of aircraft operators surveyed believe that a helpline or other mechanism should be established to assist with the implementation of VPESP. TSA asked the aircraft operators what mechanism should be established if they responded “yes” and why a mechanism should not be established if they responded “no.” The study yielded a variety of responses which are outlined in Table 8 below. To supplement this review, TSA asked aircraft operators if they provided any type of VPESP reference materials at airports served by their airline. Responses to this question are outlined in Table 9.

Table 8: Establishment of a VPESP Helpline or other Mechanism

Should a Helpline or other Mechanism be Established?	
YES: 19 (29%)	NO: 47 (71%)
What Should be Done?	Why Not?
# that added VPESP as part of their internal helpdesk: 6	# that have VPESP as part of their internal helpdesk: 11
# that stated TSA should provide training: 4	# that believe VPESP is unnecessary/no benefit: 10
# that did not specify how: 3	# that place information in service manual: 7
# that stated TSA should provide hotline: 3	# that state process is simple enough: 5
# that stated info should be on TSA's Web site: 2	# that make information available at airports: 5
# that stated TSA should produce signs: 1	# that expect employees to know information: 4
	# that place information on company intranet: 3
	# that claim internal helpline is in development: 1
	# that did not provide a response: 1

Table 9: Available Reference Material

Does the Aircraft Operator Provide Reference Materials at the Airports It Serves?	
YES: 46 (70%)	NO: 20 (30%)

A majority of aircraft operators believed a helpline or other mechanism was not necessary. Over 50 percent of aircraft operators who responded “no” stated that this information is readily available via a company helpline, intranet, or service manual and that any additional mechanism would be unnecessary and redundant. Five of the aircraft operators that responded “no” believed the process was simple and did not justify the need or cost of a hotline or similar mechanism. All five of these carriers exceed current requirements and conduct VPESP training in a classroom environment, which they likely deem sufficient. Four aircraft operators expect their employees to know VPESP as part of their daily responsibilities. This position appears justified considering these four aircraft operators exceed current requirements and conduct VPESP training on an annual recurrent schedule. One remaining aircraft operator failed to provide a reason. Only 19 aircraft operators responded that a helpline or other mechanism should be established. Six of these took the initiative and added the VPESP requirements to their internal helpdesk available to all employees.

Overall, it is encouraging that 46 aircraft operators provide employees with resources to assist with implementing VPESP as noted in Table 9. However, this number can and should be greater. Seven aircraft operators that provide resources believed TSA should

provide employee training or develop a helpline that employees could utilize. TSA disagrees with this assessment. The aircraft operator is always responsible for making sure that its employees are aware of and comply with regulatory requirements. Furthermore, the aircraft operator may contact its assigned PSI for assistance if its employees are confused about VPESP requirements. Accordingly, a TSA helpline is unnecessary. Of the remaining six aircraft operators that responded “yes,” three did not provide any further recommendations on the type of mechanism they believed appropriate. Two believed that TSA should post VPESP program information on its website, and TSA plans to do so in accordance with the Explanatory Statement for the FY08 Act. One aircraft operator believed that TSA should produce signage for placing in airport lobbies. TSA disagrees with this proposal and does not believe that it should incur a cost for a program that is required to be implemented by the aircraft operators.

Action Items

Given the results of the study, TSA has developed the following action items to assist with implementing VPESP and to increase aircraft operator compliance with the program.

Item #1: Have PSIs contact each of their assigned aircraft operators to: (1) reinforce the purpose of VPESP; (2) verify that VPESP is implemented at all domestic locations served by the aircraft operator; (3) clarify that failure to implement VPESP may subject the aircraft operator to enforcement action; and (4) answer any questions or clarify any confusion with VPESP.

As the primary liaison between TSA and the aircraft operator, the PSI is the most appropriate individual to reinforce the importance of VPESP. By working directly with the aircraft operator corporate security departments, the PSI can verify that VPESP is implemented properly and uniformly at all domestic locations served by the airline. TSA will take enforcement action, when necessary, for non-compliance with VPESP.

Item #2: Strongly encourage the aircraft operator to provide employees reference material at all domestic airports served by the airline.

TSA is encouraged by the number of aircraft operators that currently provide employees VPESP reference material, whether via a helpdesk, the company’s intranet, or a bulletin or manual. Having this type of material readily available at all domestic airports served by the aircraft operator will assist with proper VPESP implementation and ensure greater compliance with the program.

Item #3: Incorporate VPESP requirements into the Ground Security Coordinator (GSC) training curriculum for increased awareness of the program.

Aircraft operators are required to have at least one GSC available for each departing flight or when any security measure required by the AOSSP is performed. Typically, aircraft operators train many of their employees to become GSCs, so numerous GSC-

certified employees are available at each location they serve. Since these individuals are readily available to employees, incorporating VPESP training into their curriculum will increase the number of people at airports who are readily familiar with the program. Having GSCs trained to VPESP requirements can only further increase awareness with the program at any location served by an aircraft operator.

Conclusion

As previously stated in our March 26, 2007 report to Congress on VPESP, TSA believes that VPESP provides an additional level of safety to aircraft passengers by allowing qualified individuals to utilize their expertise and assist flight crews in the event of an emergency. Additionally, it gives liability protection to qualified individuals who assist during an in-flight emergency. While aircraft operators have already developed methods and contingency plans to address onboard emergencies, VPESP can increase the availability of an expedited response to certain onboard situations.

Since September 11, 2001, a number of programs have been developed to address security incidents onboard aircraft. These programs include, but are not limited to, enhanced crewmember training to address specific threats, implementation of the Federal Flight Deck Officer program, and increases in the number of Federal Air Marshals and other federal law enforcement officers on flights. These individuals are trained to be the first responders onboard aircraft should a security incident arise. While qualified individuals could prove helpful in these situations, they do not receive the type of training provided to these first responders to specifically address security related situations during flight. However, the program augments emergency procedures already established by aircraft operators and offers crewmembers additional options during an in-flight emergency.

TSA will ensure that the report previously submitted to Congress on March 26, 2007, as well as this report, are published on TSA's internet website. TSA will also develop a mechanism for reporting problems with or submitting comments on VPESP on TSA's internet website.



***The Transportation Security Administration's
Report to Congress
On a
Sterile Area Access System***

**In Accordance with the Implementing
Recommendations of the 9/11 Commission Act of 2007
(P.L. 110-53)**

March 2008

Introduction

The Implementing Recommendations of the 9/11 Commission Act of 2007 ("the 9/11 Act"), Public Law 110-53, signed on August 3, 2007, directs the Transportation Security Administration (TSA) to submit a report on its efforts to institute a sterile area access system or method that validates the identity of and expedites the screening process for working flight deck and cabin crewmembers. Specifically, Section 1614 of the Act states:

(a) Report- Not later than 180 days after the date of enactment of this Act, the Administrator of the Transportation Security Administration, after consultation with airline, airport, and flight crew representatives, shall submit to the Committee on Commerce, Science, and Transportation of the Senate, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Homeland Security of the House of Representatives, and the Committee on Transportation and Infrastructure of the House of Representatives a report on the status of the Administration's efforts to institute a sterile area access system or method that will enhance security by properly identifying authorized airline flight deck and cabin crew members at screening checkpoints and granting them expedited access through screening checkpoints. The Administrator shall include in the report recommendations on the feasibility of implementing the system for the domestic aviation industry beginning 1 year after the date on which the report is submitted.

This report is submitted to Congress in compliance with this request.

Current Status of Expedited Sterile Area Access for Working Crewmembers

The process of identifying working flight deck and cabin crewmembers at security checkpoints and providing them an expedited screening experience is partially established. Currently there are two primary methods to accelerate the screening process for crewmembers.¹ The first method is the establishment of additional queues dedicated to checking the identification of working crewmembers. TSA regulations mandate that all individuals 18 years of age and older who enter the security checkpoint must have their ID validated. Typically, there is a single queue that proceeds first to the individual checking ID and then to the security checkpoint itself. Under this method crewmembers have priority access to the ID checkers and, after identifying themselves as crewmembers, proceed directly to screening.

The second method is the establishment of entirely separate security checkpoints dedicated to working crewmembers. These restricted checkpoints allow crewmembers to avoid the queues generally experienced by the traveling public. While these two processes facilitate a quicker screening experience for working crewmembers, they are not available at every airport.

Identification of crewmembers is accomplished through a visual inspection of their airline-issued ID, which at most airports now includes the use of ultraviolet lights and magnifying loupes to

¹ In some airports, airport employees who need access to the sterile area are afforded the same priority as working crewmembers. For ease of discussion, this report focuses on crewmembers only.

help detect fraud. This method enhances the ID validation process but does not capitalize on other available validation technologies or systems currently used within the industry.

Status of Efforts to Identify and Improve Sterile Area Access for Working Crewmembers

Available resources at our security checkpoints and the complexities and costs associated with technologies that reliably validate the identity of individuals have restricted TSA's ability to implement an innovative crewmember screening system. As TSA's screening processes have become more efficient, and with the implementation of technologies employed by airlines to validate the identity and employment status of crewmembers, the possibility of providing this population a sterile area access system that offers expedited screening is increasing. TSA has begun evaluating several crewmember screening proposals by organizations representing flight deck crewmembers.² Subsequent discussions with these groups demonstrate that government and industry can work together to address potential security vulnerabilities while focusing on the operational needs of working crewmembers. Since it is vital that all assets of the industry remain engaged in this commitment, TSA has created a working group of key aviation stakeholders, as required by Section 1614 of the 9/11 Act, to receive input and opinions on the evaluation and development of any proposed sterile area access system.

One of the proposals, endorsed by the Air Line Pilots Association, offers promising solutions on how to achieve this goal. Central to this proposal is TSA's ability to leverage the success of the Cockpit Access Security System (CASS), implemented in 2005 to enhance the approval of off-line flight deck crewmembers' requests to ride the jump seat on aircraft flown by other airlines. CASS is highly praised and employed by over 85 U.S. domestic airlines.

CASS enables aircraft operators to validate reliably the identity and employment status of off-line flight deck crewmembers from other airlines that request jump seat access on one of their aircraft. Airlines participating in the CASS program maintain a database of their flight deck crewmembers that are authorized to ride the jump seat. These databases are interconnected so gate agents can query the personal records of flight deck crewmembers requesting to ride the jump seat. A flight deck crewmember provides the gate agent with requisite information, which the gate agent enters into CASS. CASS presents the gate agent with an "accept" or "deny" response, based on the crewmember's employment status, and a full-color picture to validate his or her identity. When a flight deck crewmember's employment is terminated, the carrier he or she worked for is responsible for immediately removing the crewmember's name from its database; if that individual requests jump seat access, CASS sends a "deny" response to a gate agent's query.

CASS presents a practical foundation for a system that can validate the identity of crewmembers at screening checkpoints. The system is readily available, widely and successfully used, and accessible with a standard internet connection and web browser, limiting the need for extensive and potentially costly hardware. The system provides a security layer by confirming information provided by the crewmember and providing the gate agent with an electronic color photograph for validating the identity of crewmember requesting to ride jumpseat.

² These associations are the Air Line Pilots Association and the Coalition of Air Line Pilots Association

However, CASS does have limitations, which must be further evaluated. Currently, CASS is only available to validate the identity and employment status of flight deck crewmembers; a similar system has not been instituted for cabin crewmembers since they are not authorized to ride the jump seat. TSA intends to pilot and possibly to institute a system that will provide expedited sterile access area for *all* traveling crewmembers, as is required by section 1614 of the 9/11 Act. In addition, there is debate on whether biometric technologies would be more appropriate than CASS for a sterile area access system. Biometric technologies that scan an iris or fingerprint can accurately validate an individual and are less subject to fraud; however, they generally are more expensive and difficult to maintain.

Another concern is the availability, or lack thereof, of space at federalized airports across the country. In several cases, airport facilities are struggling to accommodate growing passenger levels while ensuring enough room for required security checkpoints. Any sterile area access system for crewmembers will likely be conducted at a security checkpoint since sterile area access is almost entirely provided through these areas. The ability to accommodate such a system, including expedited screening procedures, could prove to be very challenging. While capacity constraints are evident at larger airports across the country, they create even greater problems at smaller airports that are rapidly growing through increased flight operations and the resulting increase in passenger traffic.

Despite these limitations and concerns, TSA remains committed to developing innovative systems that can validate the identity of working crewmembers at the screening checkpoint and provide them expedited access to the sterile area. TSA is actively pursuing the possibility of implementing a sterile area access system that utilizes CASS as a platform to validate the identity of working crewmembers at the security checkpoint. Part of this evaluation will assess the feasibility of extending this technology to cabin crewmembers. Some industry stakeholders believe CASS could accommodate the cabin crewmember population through hardware and software updates. However, this cannot be done without additional personnel and cost, including the cost to participating carriers of uploading their entire cabin crewmember roster and information into the CASS database. The use of technology to validate the identity of crewmembers will also require additional personnel to perform the validation process and to ensure the system is operating properly.

In addition to our evaluation of CASS for validating crewmember identity, TSA is investigating whether this technology can augment a screening process that provides expedited access to the sterile area. This presents a greater challenge because TSA must weigh the need for security against the operational demands of accommodating traveling crewmembers. Some stakeholders remain dissatisfied with current screening methods that subject vetted crewmembers to the same screening standards as the traveling public. Some scrutiny of crewmembers is necessary because they work in the sensitive aviation environment. In view of the numerous background investigations to which these individuals are subjected and their operational requirements, TSA does provide crewmembers with certain allowances not provided to the traveling public. For example, crewmembers are exempt from the current liquid, gels, and aerosols prohibition. TSA is determining whether these allowances could serve as a foundation for screening system that provides expedited access to the sterile area through the screening checkpoint.

Recommendations and Conclusions

Given the complexity of the issue, TSA will test the feasibility of proposed sterile access systems before widely instituting them on a pilot basis at select airports. Given the technology, resource, and spatial constraints, an expectation that a single crewmember screening system could easily be implemented at all federalized airports is impractical. Pilot testing will allow TSA to test concepts within these limitations and provide the opportunity to adjust or enhance any system to make wider deployment feasible. Should TSA determine that a sterile area access system's benefits outweigh the cost, these systems will be deployed on a case by case basis to airports that demonstrate the greatest need for and can accommodate such a system. TSA plans to deploy a pilot sterile area access system at multiple airports in calendar year 2008.

Conversely, TSA will recommend against implementing a sterile area access system if it determines through pilot development and testing that the costs and burdens of implementing such a system do not justify the benefits. Should TSA determine that a crewmember screening system is not feasible at this time, we will continue to evaluate the issue as screening processes and technologies evolve.

TSA strives to set standards for excellence in transportation security through its people, processes, and technology. We are looking forward to continuing our work with aviation stakeholders to develop, evaluate, and potentially deploy a sterile area access system that validates the identity of crewmembers entering the screening checkpoint and provides expedited access to the sterile area.

MAR 26 2008

Office of Legislative Affairs

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



**Homeland
Security**

The Honorable James L. Oberstar
Chairman
Committee on Transportation and Infrastructure
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

The enclosed document constitutes the Transportation Security Administration's (TSA) report regarding its efforts to institute a sterile area access system or method that verifies the identity of and expedites the screening process for working flight deck and cabin crewmembers as required by the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, section 1614, signed on August 3, 2007.

The report details TSA's current efforts to institute a sterile area access system or method that will enhance security by properly identifying authorized airline flight deck and cabin crew members at screening checkpoints and granting them expedited access through screening checkpoints into the sterile area. The report details current proposals for a sterile area access system that are under review; TSA's determination of the feasibility of implementing the aforementioned system within 1 year after the report submission deadline; and the challenges the agency will face instituting this type of system.

An identical letter has been sent to the Vice Chairman of the Senate Committee on Commerce, Science and Transportation, as well as the Chairmen and Ranking Members of the Senate Committee on Homeland Security and Governmental Affairs, the House Committee on Transportation and Infrastructure, and the House Committee on Homeland Security.

I appreciate your interest in the Department of Homeland Security, and I look forward to working with you on future homeland security issues. If I may be of further assistance, please contact the Office of Legislative Affairs at (202) 447-5890.

Sincerely,

A handwritten signature in black ink, appearing to read "Donald H. Kent, Jr.", with a stylized flourish at the end.

Donald H. Kent, Jr.
Assistant Secretary
Office of Legislative Affairs

Enclosure

MAR 26 2008



**Homeland
Security**

The Honorable John L. Mica
Ranking Member
Committee on Transportation and Infrastructure
U.S. House of Representatives
Washington, DC 20515

Dear Representative Mica:

The enclosed document constitutes the Transportation Security Administration's (TSA) report regarding its efforts to institute a sterile area access system or method that verifies the identity of and expedites the screening process for working flight deck and cabin crewmembers as required by the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, section 1614, signed on August 3, 2007.

The report details TSA's current efforts to institute a sterile area access system or method that will enhance security by properly identifying authorized airline flight deck and cabin crew members at screening checkpoints and granting them expedited access through screening checkpoints into the sterile area. The report details current proposals for a sterile area access system that are under review; TSA's determination of the feasibility of implementing the aforementioned system within 1 year after the report submission deadline; and the challenges the agency will face instituting this type of system.

An identical letter has been sent to the Vice Chairman of the Senate Committee on Commerce, Science and Transportation, as well as the Chairmen and Ranking Members of the Senate Committee on Homeland Security and Governmental Affairs, the House Committee on Transportation and Infrastructure, and the House Committee on Homeland Security.

I appreciate your interest in the Department of Homeland Security, and I look forward to working with you on future homeland security issues. If I may be of further assistance, please contact the Office of Legislative Affairs at (202) 447-5890.

Sincerely,

A handwritten signature in black ink, appearing to read "Don Kent".

Donald H. Kent, Jr.
Assistant Secretary
Office of Legislative Affairs

Enclosure

Office of Legislative Affairs

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

MAR 23 2008



**Homeland
Security**

The Honorable Daniel K. Inouye
Chairman
Committee on Commerce, Science
and Transportation
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

The enclosed document constitutes the Transportation Security Administration's (TSA) report regarding its efforts to institute a sterile area access system or method that verifies the identity of and expedites the screening process for working flight deck and cabin crewmembers as required by the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, section 1614, signed on August 3, 2007.

The report details TSA's current efforts to institute a sterile area access system or method that will enhance security by properly identifying authorized airline flight deck and cabin crew members at screening checkpoints and granting them expedited access through screening checkpoints into the sterile area. The report details current proposals for a sterile area access system that are under review; TSA's determination of the feasibility of implementing the aforementioned system within 1 year after the report submission deadline; and the challenges the agency will face instituting this type of system.

An identical letter has been sent to the Vice Chairman of the Senate Committee on Commerce, Science and Transportation, as well as the Chairmen and Ranking Members of the Senate Committee on Homeland Security and Governmental Affairs, the House Committee on Transportation and Infrastructure, and the House Committee on Homeland Security.

I appreciate your interest in the Department of Homeland Security, and I look forward to working with you on future homeland security issues. If I may be of further assistance, please contact the Office of Legislative Affairs at (202) 447-5890.

Sincerely,

A handwritten signature in black ink, appearing to read "Don Kent".

Donald H. Kent, Jr.
Assistant Secretary
Office of Legislative Affairs

Enclosure

MAR 26 2008



Homeland
Security

The Honorable Joseph I. Lieberman
Chairman
Committee on Homeland Security
and Governmental Affairs
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

The enclosed document constitutes the Transportation Security Administration's (TSA) report regarding its efforts to institute a sterile area access system or method that verifies the identity of and expedites the screening process for working flight deck and cabin crewmembers as required by the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, section 1614, signed on August 3, 2007.

The report details TSA's current efforts to institute a sterile area access system or method that will enhance security by properly identifying authorized airline flight deck and cabin crew members at screening checkpoints and granting them expedited access through screening checkpoints into the sterile area. The report details current proposals for a sterile area access system that are under review; TSA's determination of the feasibility of implementing the aforementioned system within 1 year after the report submission deadline; and the challenges the agency will face instituting this type of system.

An identical letter has been sent to the Vice Chairman of the Senate Committee on Commerce, Science and Transportation, as well as the Chairmen and Ranking Members of the Senate Committee on Homeland Security and Governmental Affairs, the House Committee on Transportation and Infrastructure, and the House Committee on Homeland Security.

I appreciate your interest in the Department of Homeland Security, and I look forward to working with you on future homeland security issues. If I may be of further assistance, please contact the Office of Legislative Affairs at (202) 447-5890.

Sincerely,

A handwritten signature in black ink, appearing to read "Don Kent".

Donald H. Kent, Jr.
Assistant Secretary
Office of Legislative Affairs

Enclosure

MAR 26 2008

Office of Legislative Affairs

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



**Homeland
Security**

The Honorable Susan M. Collins
Ranking Member
Committee on Homeland Security
and Governmental Affairs
United States Senate
Washington, DC 20510

Dear Senator Collins:

The enclosed document constitutes the Transportation Security Administration's (TSA) report regarding its efforts to institute a sterile area access system or method that verifies the identity of and expedites the screening process for working flight deck and cabin crewmembers as required by the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, section 1614, signed on August 3, 2007.

The report details TSA's current efforts to institute a sterile area access system or method that will enhance security by properly identifying authorized airline flight deck and cabin crew members at screening checkpoints and granting them expedited access through screening checkpoints into the sterile area. The report details current proposals for a sterile area access system that are under review; TSA's determination of the feasibility of implementing the aforementioned system within 1 year after the report submission deadline; and the challenges the agency will face instituting this type of system.

An identical letter has been sent to the Vice Chairman of the Senate Committee on Commerce, Science and Transportation, as well as the Chairmen and Ranking Members of the Senate Committee on Homeland Security and Governmental Affairs, the House Committee on Transportation and Infrastructure, and the House Committee on Homeland Security.

I appreciate your interest in the Department of Homeland Security, and I look forward to working with you on future homeland security issues. If I may be of further assistance, please contact the Office of Legislative Affairs at (202) 447-5890.

Sincerely,

A handwritten signature in black ink, appearing to read "Don Kent".

Donald H. Kent, Jr.
Assistant Secretary
Office of Legislative Affairs

Enclosure

MAR 26 2008

Office of Legislative Affairs

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



**Homeland
Security**

The Honorable Peter T. King
Ranking Member
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

Dear Representative King:

The enclosed document constitutes the Transportation Security Administration's (TSA) report regarding its efforts to institute a sterile area access system or method that verifies the identity of and expedites the screening process for working flight deck and cabin crewmembers as required by the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, section 1614, signed on August 3, 2007.

The report details TSA's current efforts to institute a sterile area access system or method that will enhance security by properly identifying authorized airline flight deck and cabin crew members at screening checkpoints and granting them expedited access through screening checkpoints into the sterile area. The report details current proposals for a sterile area access system that are under review; TSA's determination of the feasibility of implementing the aforementioned system within 1 year after the report submission deadline; and the challenges the agency will face instituting this type of system.

An identical letter has been sent to the Vice Chairman of the Senate Committee on Commerce, Science and Transportation, as well as the Chairmen and Ranking Members of the Senate Committee on Homeland Security and Governmental Affairs, the House Committee on Transportation and Infrastructure, and the House Committee on Homeland Security.

I appreciate your interest in the Department of Homeland Security, and I look forward to working with you on future homeland security issues. If I may be of further assistance, please contact the Office of Legislative Affairs at (202) 447-5890.

Sincerely,

A handwritten signature in black ink, appearing to read "D. Kent".

Donald H. Kent, Jr.
Assistant Secretary
Office of Legislative Affairs

Enclosure

MAR 26 2008

Office of Legislative Affairs

U.S. Department of Homeland Security
Washington, DC 20523



**Homeland
Security**

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

The enclosed document constitutes the Transportation Security Administration's (TSA) report regarding its efforts to institute a sterile area access system or method that verifies the identity of and expedites the screening process for working flight deck and cabin crewmembers as required by the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, section 1614, signed on August 3, 2007.

The report details TSA's current efforts to institute a sterile area access system or method that will enhance security by properly identifying authorized airline flight deck and cabin crew members at screening checkpoints and granting them expedited access through screening checkpoints into the sterile area. The report details current proposals for a sterile area access system that are under review; TSA's determination of the feasibility of implementing the aforementioned system within 1 year after the report submission deadline; and the challenges the agency will face instituting this type of system.

An identical letter has been sent to the Vice Chairman of the Senate Committee on Commerce, Science and Transportation, as well as the Chairmen and Ranking Members of the Senate Committee on Homeland Security and Governmental Affairs, the House Committee on Transportation and Infrastructure, and the House Committee on Homeland Security.

I appreciate your interest in the Department of Homeland Security, and I look forward to working with you on future homeland security issues. If I may be of further assistance, please contact the Office of Legislative Affairs at (202) 447-5890.

Sincerely,

A handwritten signature in black ink, appearing to read "Don Kent".

Donald H. Kent, Jr.
Assistant Secretary
Office of Legislative Affairs

Enclosure

Office of Legislative Affairs

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

MAR 26 2008



**Homeland
Security**

The Honorable Ted Stevens
Vice Chairman
Committee on Commerce, Science
and Transportation
United States Senate
Washington, DC 20510

Dear Senator Stevens:

The enclosed document constitutes the Transportation Security Administration's (TSA) report regarding its efforts to institute a sterile area access system or method that verifies the identity of and expedites the screening process for working flight deck and cabin crewmembers as required by the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, section 1614, signed on August 3, 2007.

The report details TSA's current efforts to institute a sterile area access system or method that will enhance security by properly identifying authorized airline flight deck and cabin crew members at screening checkpoints and granting them expedited access through screening checkpoints into the sterile area. The report details current proposals for a sterile area access system that are under review; TSA's determination of the feasibility of implementing the aforementioned system within 1 year after the report submission deadline; and the challenges the agency will face instituting this type of system.

An identical letter has been sent to the Vice Chairman of the Senate Committee on Commerce, Science and Transportation, as well as the Chairmen and Ranking Members of the Senate Committee on Homeland Security and Governmental Affairs, the House Committee on Transportation and Infrastructure, and the House Committee on Homeland Security.

I appreciate your interest in the Department of Homeland Security, and I look forward to working with you on future homeland security issues. If I may be of further assistance, please contact the Office of Legislative Affairs at (202) 447-5890.

Sincerely,

A handwritten signature in black ink, appearing to read "Don Kent".

Donald H. Kent, Jr.
Assistant Secretary
Office of Legislative Affairs

Enclosure



*The Transportation Security Administration's
Report to Congress
On a
Sterile Area Access System*

**In Accordance with the Implementing
Recommendations of the 9/11 Commission Act of 2007
(P.L. 110-53)**

March 2008

Introduction

The Implementing Recommendations of the 9/11 Commission Act of 2007 ("the 9/11 Act"), Public Law 110-53, signed on August 3, 2007, directs the Transportation Security Administration (TSA) to submit a report on its efforts to institute a sterile area access system or method that validates the identity of and expedites the screening process for working flight deck and cabin crewmembers. Specifically, Section 1614 of the Act states:

(a) Report- Not later than 180 days after the date of enactment of this Act, the Administrator of the Transportation Security Administration, after consultation with airline, airport, and flight crew representatives, shall submit to the Committee on Commerce, Science, and Transportation of the Senate, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Homeland Security of the House of Representatives, and the Committee on Transportation and Infrastructure of the House of Representatives a report on the status of the Administration's efforts to institute a sterile area access system or method that will enhance security by properly identifying authorized airline flight deck and cabin crew members at screening checkpoints and granting them expedited access through screening checkpoints. The Administrator shall include in the report recommendations on the feasibility of implementing the system for the domestic aviation industry beginning 1 year after the date on which the report is submitted.

This report is submitted to Congress in compliance with this request.

Current Status of Expedited Sterile Area Access for Working Crewmembers

The process of identifying working flight deck and cabin crewmembers at security checkpoints and providing them an expedited screening experience is partially established. Currently there are two primary methods to accelerate the screening process for crewmembers.¹ The first method is the establishment of additional queues dedicated to checking the identification of working crewmembers. TSA regulations mandate that all individuals 18 years of age and older who enter the security checkpoint must have their ID validated. Typically, there is a single queue that proceeds first to the individual checking ID and then to the security checkpoint itself. Under this method crewmembers have priority access to the ID checkers and, after identifying themselves as crewmembers, proceed directly to screening.

The second method is the establishment of entirely separate security checkpoints dedicated to working crewmembers. These restricted checkpoints allow crewmembers to avoid the queues generally experienced by the traveling public. While these two processes facilitate a quicker screening experience for working crewmembers, they are not available at every airport.

Identification of crewmembers is accomplished through a visual inspection of their airline-issued ID, which at most airports now includes the use of ultraviolet lights and magnifying loupes to

¹ In some airports, airport employees who need access to the sterile area are afforded the same priority as working crewmembers. For ease of discussion, this report focuses on crewmembers only.

help detect fraud. This method enhances the ID validation process but does not capitalize on other available validation technologies or systems currently used within the industry.

Status of Efforts to Identify and Improve Sterile Area Access for Working Crewmembers

Available resources at our security checkpoints and the complexities and costs associated with technologies that reliably validate the identity of individuals have restricted TSA's ability to implement an innovative crewmember screening system. As TSA's screening processes have become more efficient, and with the implementation of technologies employed by airlines to validate the identity and employment status of crewmembers, the possibility of providing this population a sterile area access system that offers expedited screening is increasing. TSA has begun evaluating several crewmember screening proposals by organizations representing flight deck crewmembers.² Subsequent discussions with these groups demonstrate that government and industry can work together to address potential security vulnerabilities while focusing on the operational needs of working crewmembers. Since it is vital that all assets of the industry remain engaged in this commitment, TSA has created a working group of key aviation stakeholders, as required by Section 1614 of the 9/11 Act, to receive input and opinions on the evaluation and development of any proposed sterile area access system.

One of the proposals, endorsed by the Air Line Pilots Association, offers promising solutions on how to achieve this goal. Central to this proposal is TSA's ability to leverage the success of the Cockpit Access Security System (CASS), implemented in 2005 to enhance the approval of off-line flight deck crewmembers' requests to ride the jump seat on aircraft flown by other airlines. CASS is highly praised and employed by over 85 U.S. domestic airlines.

CASS enables aircraft operators to validate reliably the identity and employment status of off-line flight deck crewmembers from other airlines that request jump seat access on one of their aircraft. Airlines participating in the CASS program maintain a database of their flight deck crewmembers that are authorized to ride the jump seat. These databases are interconnected so gate agents can query the personal records of flight deck crewmembers requesting to ride the jump seat. A flight deck crewmember provides the gate agent with requisite information, which the gate agent enters into CASS. CASS presents the gate agent with an "accept" or "deny" response, based on the crewmember's employment status, and a full-color picture to validate his or her identity. When a flight deck crewmember's employment is terminated, the carrier he or she worked for is responsible for immediately removing the crewmember's name from its database; if that individual requests jump seat access, CASS sends a "deny" response to a gate agent's query.

CASS presents a practical foundation for a system that can validate the identity of crewmembers at screening checkpoints. The system is readily available, widely and successfully used, and accessible with a standard internet connection and web browser, limiting the need for extensive and potentially costly hardware. The system provides a security layer by confirming information provided by the crewmember and providing the gate agent with an electronic color photograph for validating the identity of crewmember requesting to ride jumpseat.

² These associations are the Air Line Pilots Association and the Coalition of Air Line Pilots Association

However, CASS does have limitations, which must be further evaluated. Currently, CASS is only available to validate the identity and employment status of flight deck crewmembers; a similar system has not been instituted for cabin crewmembers since they are not authorized to ride the jump seat. TSA intends to pilot and possibly to institute a system that will provide expedited sterile access area for *all* traveling crewmembers, as is required by section 1614 or the 9/11 Act. In addition, there is debate on whether biometric technologies would be more appropriate than CASS for a sterile area access system. Biometric technologies that scan an iris or fingerprint can accurately validate an individual and are less subject to fraud; however, they generally are more expensive and difficult to maintain.

Another concern is the availability, or lack thereof, of space at federalized airports across the country. In several cases, airport facilities are struggling to accommodate growing passenger levels while ensuring enough room for required security checkpoints. Any sterile area access system for crewmembers will likely be conducted at a security checkpoint since sterile area access is almost entirely provided through these areas. The ability to accommodate such a system, including expedited screening procedures, could prove to be very challenging. While capacity constraints are evident at larger airports across the country, they create even greater problems at smaller airports that are rapidly growing through increased flight operations and the resulting increase in passenger traffic.

Despite these limitations and concerns, TSA remains committed to developing innovative systems that can validate the identity of working crewmembers at the screening checkpoint and provide them expedited access to the sterile area. TSA is actively pursuing the possibility of implementing a sterile area access system that utilizes CASS as a platform to validate the identity of working crewmembers at the security checkpoint. Part of this evaluation will assess the feasibility of extending this technology to cabin crewmembers. Some industry stakeholders believe CASS could accommodate the cabin crewmember population through hardware and software updates. However, this cannot be done without additional personnel and cost, including the cost to participating carriers of uploading their entire cabin crewmember roster and information into the CASS database. The use of technology to validate the identity of crewmembers will also require additional personnel to perform the validation process and to ensure the system is operating properly.

In addition to our evaluation of CASS for validating crewmember identity, TSA is investigating whether this technology can augment a screening process that provides expedited access to the sterile area. This presents a greater challenge because TSA must weigh the need for security against the operational demands of accommodating traveling crewmembers. Some stakeholders remain dissatisfied with current screening methods that subject vetted crewmembers to the same screening standards as the traveling public. Some scrutiny of crewmembers is necessary because they work in the sensitive aviation environment. In view of the numerous background investigations to which these individuals are subjected and their operational requirements, TSA does provide crewmembers with certain allowances not provided to the traveling public. For example, crewmembers are exempt from the current liquid, gels, and aerosols prohibition. TSA is determining whether these allowances could serve as a foundation for screening system that provides expedited access to the sterile area through the screening checkpoint.

Recommendations and Conclusions

Given the complexity of the issue, TSA will test the feasibility of proposed sterile access systems before widely instituting them on a pilot basis at select airports. Given the technology, resource, and spatial constraints, an expectation that a single crewmember screening system could easily be implemented at all federalized airports is impractical. Pilot testing will allow TSA to test concepts within these limitations and provide the opportunity to adjust or enhance any system to make wider deployment feasible. Should TSA determine that a sterile area access system's benefits outweigh the cost, these systems will be deployed on a case by case basis to airports that demonstrate the greatest need for and can accommodate such a system. TSA plans to deploy a pilot sterile area access system at multiple airports in calendar year 2008.

Conversely, TSA will recommend against implementing a sterile area access system if it determines through pilot development and testing that the costs and burdens of implementing such a system do not justify the benefits. Should TSA determine that a crewmember screening system is not feasible at this time, we will continue to evaluate the issue as screening processes and technologies evolve.

TSA strives to set standards for excellence in transportation security through its people, processes, and technology. We are looking forward to continuing our work with aviation stakeholders to develop, evaluate, and potentially deploy a sterile area access system that validates the identity of crewmembers entering the screening checkpoint and provides expedited access to the sterile area.



Transportation Security Administration

Implementation of Title XIV of the
Implementing Recommendations of the 9/11 Commission
Act of 2007 and the State of Public Transportation Security

January 2009

Executive Summary

This report is provided as required by Section 1412 of Title XIV (Public Transportation Security) of the *Implementing Recommendations of the 9/11 Commission Act of 2007* (9/11 Act). Section 1412 requires the Department of Homeland Security (DHS) to submit a report not later than March 31st of each year that contains the following information:

- a description of the implementation of the provisions of Title XIV;
- the amount of funds appropriated to carry out the provisions of Title XIV that have not been expended or obligated;
- the National Strategy for Public Transportation Security required under Section 1404;
- an estimate of the cost to implement the National Strategy for Public Transportation Security, which shall break out the aggregated total cost of needed capital and operational security improvements for fiscal years (FY) 2008-2018; and
- the state of public transportation security in the United States, which is to include numerous data points identified in paragraph (a) (2) (E) of Section 1412.

This report presents a summary of the status of implementation for each provision of Title XIV identified in sections 1404-1415.

The existing Mass Transit Annex to the Transportation Systems Sector Specific Plan (TS-SSP), developed pursuant to Homeland Security Presidential Directive-7, serves as the National Strategy for Public Transportation Security (Section 1404). The Annex has been developed and implemented to serve as the strategic plan for security enhancement in mass transit and passenger rail. The Annex is currently being reviewed for any necessary revisions to reflect progress in meeting strategic security priorities, update security enhancement objectives, and ensure the specific requirements of sections 1404 and 1511 (passenger rail) are included. The goal is to complete updating of the Annex during the first quarter of calendar year 2009.

Multiple programs and activities demonstrate how the Transportation Security Administration (TSA) is implementing the provisions of section 1405 on Security Assessments and Plans. For example:

- The Baseline Assessment for Security Enhancement (BASE) program has completed 88 assessments including 48 of the largest 50 mass transit and passenger rail agencies, 30 on those ranked 51-100 in size, and 10 on smaller agencies. These assessments inform the determination of security priorities, the development and implementation of security enhancement programs, and resource allocations;
- The Transit Security Grant Program (TSGP) meets the requirement in Section 1406 for Public Transportation Security Assistance. The program awarded \$343 million in FY 2008 to enhance security in eligible mass transit and passenger

rail systems. An additional \$25 million went to Amtrak. In FY 2009, the TSGP will award \$348 million to eligible mass transit and passenger rail systems, plus another \$25 million to Amtrak;

- Progress in advancing security exercises in mass transit and passenger rail (Section 1407) occurred through a pilot initiative in the National Capital Region of a multi-agency, cross-functional terrorism prevention and immediate response exercise program. This program adapts the Port Security Training and Exercise Program (PortSTEP) concept to surface modes of transportation. The Intermodal Security Training and Exercise Program (I-STEP) program employs a multi-phased, multi-jurisdictional, and scenario-based approach to evaluate and enhance anti-terrorism and immediate response capabilities. TSA applied the program in a joint exercise for mass transit/passenger rail agencies and freight rail carriers, with regional security partners, in northern New Jersey in September 2008. I-STEP exercises in mass transit and passenger rail are projected Seattle and Los Angeles in 2009;
- The vital importance of training frontline employees led TSA to implement a focused security training initiative under the TSGP in 2007. This program is discussed in the report on status of implementation of Section 1408, Public Transportation Security Training Program;
- DHS has established a multi-faceted process to ensure timely notification of threats, incidents, and related security concerns. These intelligence sharing means are discussed in the status report on Section 1410, Information Sharing; and
- Brief discussions on other provisions include threat assessments, public transportation employee protections, security background checks of covered individuals for public transportation, and limitations of fines and civil penalties are provided.

At this time, there are no appropriated funds that have not been expended or obligated within the period of availability for use to carry out the provisions of Title XIV.

TSA will provide appropriate cost estimates for implementation of the Public Transportation Security Strategy separately through the broader budgetary processes for DHS as coordinated by the Office of Management and Budget.

The section of this report that discusses the state of public transportation security is presented through TSA's efforts to assist public transit agencies and passenger rail carriers to deter terrorism and minimize the effects of terrorist attacks. The numerous programs, activities, and initiatives discussed are organized under each of the five guiding principles that provide the foundation for the TSA mass transit security program. The five principles are: 1) expanding partnerships for security enhancement; 2) elevating the security baseline; 3) building security force multipliers; 4) leading information assurance; and 5) protecting high risk assets and systems. This multi-faceted effort aims to produce sustainable collaboration among TSA and security partners in Federal, State,

and local government and mass transit and passenger rail agencies and implement effective layers of security.

Background

In pertinent part, Section 1412 requires that, not later than March 31st of each year, DHS must report to Congress as follows:

- a description of the implementation of the provisions of title XIV
- appropriated funds for these purposes that were not expended or obligated
- implementation of the National Strategy for Public Transportation Security (NSPTS) required under section 1404
- “the state of public transportation security,” which is to include numerous data points on progress being made by public transportation agencies and differences among them.¹

I. Implementation of Provisions of Title XIV, Public Transportation Security

Section 1404 – National Strategy for Public Transportation Security: The existing Mass Transit Annex to TS-SSP, produced in coordination with the Transit, Commuter and Long Distance Rail Government Coordinating Council (GCC), Mass Transit Sector Coordinating Council (SCC), and the Transit Policing and Security Peer Advisory Group (PAG) and published in June 2007, meets the legislative requirement for a national strategy for passenger rail security. The Annex presents the coordinated security enhancement strategy for public transportation and passenger rail systems. Section 1404(e) directs use of “relevant existing plans, strategies, and risk assessments developed by the Department or other Federal agencies, including those developed or implemented pursuant to section 114(t) of title 49, United States Code, or Homeland Security Presidential Directive-7.” The Mass Transit Annex to the TS-SSP falls within the scope of this direction. The Annex has been developed and implemented to serve as the strategic plan for security enhancement in mass transit and passenger rail. Review of the Annex for any necessary updating of the discussion of strategic security priorities and their achievement, as well as to ensure specific components required by Section 1404 and the similar provision applicable to passenger rail at Section 1511 are met is ongoing. Coordination of the proposed changes and supplements began in October with the GCC, SCC, and PAG, to continue through January 2009 with the objective of completing the updated Annex for approval and publication by late March 2009.

Section 1405 – Security Assessments and Plans: Multiple actions demonstrate that TSA has made significant progress towards compliance with the provisions of this section. For example, all 37 security assessments conducted by the Federal Transit Administration (FTA) among the 50 largest mass transit agencies were provided to TSA prior to enactment of the 9/11 Act. These materials informed the development of the TSA/FTA Security and Emergency Management Action Items and the Baseline

¹ *Implementing Recommendations of the 9/11 Commission Act of 2007* (Public Law 110-53, August 3, 2007), Section 1412.

Assessment for Security Enhancement (BASE) program by which TSA assesses mass transit agencies' implementation of the Action Items.

Developed in a joint effort of TSA, DHS, Department of Transportation (DOT), and mass transit and passenger rail operating and security officials engaged through the Mass Transit SCC and Transit Policing and Security Peer Advisory Group, the Action Items cover a range of areas that are foundational to an effective security program.

Components include security program management and accountability, security and emergency response training, drills and exercises, public awareness, protective measures for Homeland Security Advisory System (HSAS) threat levels, physical security, personnel security, and information sharing and security. Particular emphasis is placed on posture in the six Transit Security Fundamentals (protection of underground/underwater infrastructure; protection of other high consequence systems and assets; random, unpredictable deterrence; training; exercises; and public awareness).

Security assessments conducted under BASE program confirm that security plans have been developed and are being implemented. To date, TSA has completed 88 BASE assessments, covering 48 of the largest 50 mass transit and passenger rail agencies, 30 on agencies ranked 51-100 in size, 10 smaller agencies. The Nation's 100 largest mass transit and passenger rail agencies account for more than 80 percent of the total users of mass transit and passenger rail systems. The results of the BASE assessments inform the determination of security priorities and the development and implementation of security enhancement programs and resource allocations.

TSA has completed security assessments under the BASE program of 29 bus-only systems. The assessment results are analyzed both by individual agency and consolidation of all bus-only systems to identify trends in areas needing improvement. This effort has contributed to the progress of a joint initiative with FTA through the Bus Safety and Security Program to produce security enhancement tools for smaller bus agencies. Coordination of this effort with small system security partners occurred at the Bus Safety and Security Conference in Dallas during March 3-5, 2008. Subsequent actions have advanced a collaborative effort to produce security action items and an assessment tool tailored to the operational circumstances of smaller bus agencies.

Concerning the mandated rulemaking to require that "high risk" agencies maintain and implement security plans, TSNM Mass Transit is proceeding with development of a summary of the developing concept for a security plan regulation for public transportation agencies. This approach was briefed to the Transit GCC in May 2008, the Mass Transit SCC in June 2008, and to the PAG during monthly teleconferences. Consultations with the public transportation community will occur through these forums, with further outreach among mass transit and passenger rail security officials, employee labor organizations, and first responder associations. These consultations will ensure that development of regulatory requirements reflects operational realities.

Section 1406 – Public Transportation Security Assistance: The existing TSGP meets the requirement of this section to "establish a program for making grants to eligible

public transportation agencies for security improvements” In compliance with a specific requirement of this section, the Secretaries of Homeland Security and Transportation completed a joint letter, dated December 21, 2007, notifying the appropriate congressional committees of their determination that retaining DHS as the lead Federal entity in substantive and administrative matters pertaining to the TSGP is the most efficient means of distribution of grant funds to mass transit and passenger rail agency recipients.

DHS published the FY 2008 program guidance published in February 2008. The TSGP continues to emphasize enhancing security posture in the six Transit Security Fundamentals (protection of underground/underwater infrastructure; protection of other high consequence systems and assets; random, unpredictable deterrence; training; exercises; and public awareness). The program guidance lists the eligible mass transit and passenger rail agencies in regions categorized by risk as Tier 1 and Tier 2 and specifies the security enhancement priorities through a listing of project effectiveness groupings. The Secretary announced the FY 2008 TSGP awards on May 16, 2008.

For the FY 2009 program, the Secretary published the grant guidance on November 5, 2008. Development of project proposals by eligible agencies is ongoing as of the date of this report. In FY 2009, the TSGP will award \$348 million to eligible mass transit and passenger rail systems, plus another \$25 million to Amtrak.

During FY 2008, the total funding allocation is \$343 million to eligible mass transit and passenger rail systems, plus \$25 million to Amtrak. Total funding under the program in FY 2007 reached \$255 million through the annual DHS appropriation and the supplemental.

Further details on the TSGP, including summaries of consultations with eligible agencies through meetings, regular teleconferences, and responses to inquiries, may be accessed through the DHS public website at: <http://www.tsa.gov/join/grants/tsgp.shtm>. Of note, TSA held two feedback sessions during September/October 2008 to afford eligible agencies and the Mass Transit SCC the opportunity to provide feedback on their experience with the TSGP and recommendations for improving the program. A western regional session took place on September 29 in Seattle and an eastern regional session in Washington, DC, on October 15.

Section 1407 - Security Exercises: TSA is advancing development of an exercise program for public transportation agencies through a pilot initiative conducted in the National Capital Region (NCR). The Intermodal Security Training and Exercise Program (I-STEP), an adaptation of the PortSTEP concept to surface modes of transportation, employs a multi-phased, multi-jurisdictional, cross-functional, and scenario-based approach to evaluate and enhance anti-terrorism and immediate response capabilities. This approach is informed by BASE assessment results indicating a need for significant expansion of terrorism prevention exercises focused on threats and incidents in a mass transit or passenger rail system.

The principal participating agencies in the NCR included TSA, Amtrak, WMATA, Maryland Transit, and Virginia Railway Express. The initial coordination forum was held in January 2008, with each of these agencies in attendance and agreeing to participate. Scenario-based anti-terrorism workshops followed over the next 3 months, with the principal agencies inviting their State and local security partners as additional participants. Coordination sessions held during May 2008 focused on preparing for the culminating event, a large scale regional table top exercise in Union Station, Washington, DC, on June 25. A joint working group has convened to develop collaborative solutions to address lessons learned in the exercise.

This program, with lessons learned from the NCR effort integrated, has been advanced as an exercise concept for application in regional areas throughout the US for adaptation to their particular operating circumstances and use in planning and conducting multi-agency, cross-functional exercises in mass transit and passenger rail. Specific emphasis is placed on enhancing and testing prevention capabilities. TSA sponsored a second I-STEP exercise for mass transit and passenger and freight rail carriers and their regional security partners in northern New Jersey in late September 2008. Planning is ongoing to conduct similar exercises in the Los Angeles and Seattle areas during the first half of 2009.

Section 1408 - Public Transportation Security Training Program: TSA is considering a multi-modal rulemaking, which would implement the security training requirements of the 9/11 Act and has been developing relevant information for each mode.

For the security training rule for mass transit and passenger rail, TSA produced a summary of the concepts under consideration to meet the statutory requirement to promulgate a regulation mandating that public transportation agencies implement security training programs. TSA shared this summary with key security partners, including the Mass Transit SCC, of which the Amalgamated Transit Union (ATU) is a member, and the PAG. Feedback from these groups has been received and is undergoing review. The input was discussed generally during a monthly teleconference with the PAG and with members of the SCC at the group's June 1, 2008, meeting in San Francisco. TSA anticipates updating the summary as appropriate based on this feedback and providing multiple constituencies an opportunity to review and provide feedback on an expedited basis. After this second round of consultations, the focus will shift to completing and publishing a notice of proposed rulemaking.

DHS recognizes the vital importance of training frontline employees. To expand the effort in this area, TSA developed and implemented a focused security training initiative under the TSGP in February 2007. TSA coordinated development of this initiative through the Mass Transit SCC and the PAG. The resulting Mass Transit Security Training Program provides guidelines to mass transit and passenger rail agencies on the types of training to be provided by category of employee. The guidance further identifies specific courses developed under Federal auspices through the FTA, the Federal Emergency Management Agency, and TSA that are available to ensure employees are

trained in the designated areas. Finally, the Department revised the eligible costs under the TSGP to allow coverage of overtime expenses incurred when employees receive training courses and streamlined the application process to simplify requests and expedite awards for security training.

This initiative has dramatically increased requests for training funds and the number of employees receiving training in such core areas as security awareness, behavior recognition, and immediate response to a threat or security incidents, areas that cover the specific components cited respectively in sections 1408 and 1517 of the 9/11 Act. As an illustrative example, the percentage of funds allocated to security training among Tier 2 systems in the TSGP increased from 3 percent of awards in FY 2006 to 68 percent of awards in FY 2007. This coordinated program, backed by Federal funding through dedicated security grants, met the Congressional objective of detailed guidelines for security training programs 6 months before enactment of the 9/11 Act.

Section 1409 – Public Transportation Research and Development: A report on the research and development program for public transportation will be submitted separately as a product of the functionally-based integrated process team approach managed by the DHS Science and Technology Directorate.

Section 1410 – Information Sharing: DHS shares intelligence with DOT through a multi-faceted process to ensure timely notification of threats, incidents, and related security concerns. This effort includes direct engagement between representatives of TSA and FTA in the interagency Mass Transit Security Information Network.

The Mass Transit Security Information Network brings together representatives from about 15 key offices within DHS and DOT, including FTA's Office of Safety and Security; TSA's Mass Transit Division, Office of Intelligence, Office of Strategic Communication and Public Affairs, Surface Transportation Security Inspection Program, Federal Air Marshal Service, and Transportation Security Operations Center; and DHS's Office of Infrastructure Protection, Office of State and Local Government Coordination, and the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC).

The Network enables informed decision-making on security measures and actions during periods of heightened threat or security incidents. It accomplishes this mission by timely development and distribution of security information products and recommendations and guidelines to mass transit and passenger rail security officials and Federal Government decision makers.

Since its establishment in August 2005, four incidents have prompted convening of the Network for these purposes: the July 2006 attacks on commuter trains in Mumbai, India; the disruption of the terror plot targeting flights from the United Kingdom bound for the United States in August 2006; the discovery of explosives in a vehicle in London and the vehicle attack on Glasgow Airport in late June 2007; and the reported threat to New York City area transit systems and terrorist attacks in Mumbai in November 2008. In each case, the Network prepared and disseminated information products that ensured mass

transit and passenger rail security officials maintained situational awareness throughout the incident. The Network provided updates on the developing situations, the security implications for the mass transit and passenger rail mode, and recommendations on security enhancement measures and activities.

TSA's Mass Transit Division provides complete copies of all Mass Transit Security Awareness Messages to mass transit and passenger rail security and law enforcement officials directly to FTA's Office of Safety and Security. Disseminated generally on a monthly basis, these Messages provide DHS, the Federal Bureau of Investigation (FBI), and TSA intelligence products with security context and recommended use in training and awareness activities to mass transit and passenger rail agencies. During 2008, subjects addressed in these Messages have included a mass transit threat assessment; suicide bomber tradecraft and planning and point of attack indicators; next generation suicide bombers and their use of elderly, female, and teenage operatives in terrorist attacks; second phase attacks to target first responders; analysis of future terrorist cells; a profile of Hezbollah; an overview of the security implications and recommended measures in light of hoax threat activity near the entrance to the Lincoln Tunnel in New Jersey; and situation reports and recommended security activities in light of the reported threat to New York City area transit systems and the terrorist attacks in Mumbai in late November 2008. With these Messages, TSA cites recommended protective measures and discusses use of the accompanying materials, which include intelligence products and training aids.

Information sharing is also achieved via alerts, advisories, and notices issued by the National Operations Center (NOC) and the Transportation Security Operations Center (TSOC). FTA's Office of Safety and Security receives these materials through notifications provided under the auspices of the Mass Transit Security Information Network as well as direct communications between the NOC and TSOC with DOT's Office of Intelligence and Security. As a representative example, during the evening of August 9-10, 2006, TSA's Mass Transit Division convened the leads from FTA's Office of Safety and Security and DHS's Office of Infrastructure Protection to inform them of the disruption of the terrorist plots targeting aircraft bound for the United States from the United Kingdom and to coordinate in preparation of an alert notification to mass transit and passenger rail law enforcement chiefs and security directors. The notification provided in the overnight hours ensured these officials were aware of the situation, the focus on aviation, and the recommendation for heightened vigilance in security activities well in advance of morning rush hours across the country. FTA's Office of Safety and Security received the alert notification and all subsequent messages related to this incident.

TSA is also involved in the development of intelligence products pertaining to public transportation. TSA's Office of Intelligence, either directly or through TSA's Mass Transit Division, consults as necessary with counterparts in the Department of Transportation's Office of Intelligence and Security or FTA's Office of Safety and Security, when developing intelligence products that pertain to public transportation.

TSA has also engaged FTA officials for participation in classified intelligence briefings on the threat to mass transit and passenger rail by two means. First, TSA's Office of Intelligence provided a briefing on the threat to mass transit to the Deputy Administrator of FTA in April 2007. Second, in partnership with DHS HITRAC and the FBI, TSA provides joint threat and analysis briefings at Secret level on a quarterly basis, bringing together mass transit and passenger rail security directors and law enforcement chiefs with their Federal security partners in 15 metropolitan areas through the secure video teleconferencing system maintained in the Joint Terrorism Task Force (JTTF) network. This capability enables timely assembly of these key officials through this means for unscheduled sessions as threats or security incidents warrant. TSA has invited regional FTA officials to participate in these sessions.

These processes are maintained and enhanced through regular coordination discussions. This effort to ensure timely and accurate situational awareness in normal operations and during periods of heightened threat or security incidents will be continuous.

The second portion of this section directs DHS to provide \$600,000 in FY 2008, FY 2009, and FY 2010 to the Information Sharing and Analysis Center for Public Transportation. TSA recognizes the importance of this legislative mandate and is committed to providing the directed support as resources permit.

Section 1411 – Threat Assessments: As an initial step, TSA determined the volume of frontline employees in public transportation agencies and assessed the scale of effort required to conduct name-based checks against the terrorist watch list and immigration status. A major challenge is developing operating procedures for collection of the names, completion of the checks, and use of the results. In view of these factors, TSA is considering a phased approach over an extended period that applies risk-based factors in prioritizing these checks by public transportation agencies.

Section 1413 – Public Transportation Employee Protections: Coordination has been completed with appropriate Department of Labor offices to ensure availability of information and materials on employee protections for reporting of security matters. The Occupational Safety and Hazards Administration public website clearly displays information pertaining to protections enacted by the 9/11 Act. This material can be accessed at <http://www.osha.gov/dep/oia/whistleblower/index.html>.

Section 1414 – Security Background Checks of Covered Individuals for Public Transportation: Guidance on conducting background checks of employees has been produced by TSA and made available by multiple means to public transportation agencies beginning in November 2007. These means include consultations with and distributions of the guidance to the Mass Transit SCC and the PAG. The guidance is also posted with the Security and Emergency Management Action Items on TSA and FTA public websites. More information on this topic can be found at: http://www.tsa.gov/assets/pdf/guidance_employee_background_checks.pdf.

Section 1415 – Limitations on Fines and Civil Penalties: The standard operating procedures for the Surface Transportation Security Inspection Program accord with the procedures set forth in this section concerning assessment of civil penalties for violations of security regulations, directives, or orders.

II. Appropriated Funds Not Expended or Obligated

None to report at this time.

III. National Strategy for Public Transportation Security

As reported above, the existing Mass Transit Annex to TS-SSP, produced in coordination with the Transit, Commuter and Long Distance Rail GCC, Mass Transit SCC, and the Transit Policing and Security PAG and published in June 2007, meets the legislative requirement for a national strategy for passenger rail security. The Annex presents the coordinated security enhancement strategy for public transportation and passenger rail systems. Section 1404(e) directs use of “relevant existing plans, strategies, and risk assessments developed by the Department or other Federal agencies, including those developed or implemented pursuant to section 114(t) of title 49, United States Code, or Homeland Security Presidential Directive-7.” The Mass Transit Annex to the TS-SSP falls within the scope of this direction. The Annex has been developed and implemented to serve as the strategic plan for security enhancement in mass transit and passenger rail. Review of the Annex for any necessary updating of the discussion of strategic security priorities and their achievement, as well as to ensure specific components required by Section 1404 and the similar provision applicable to passenger rail at Section 1511 are met is ongoing. An updated product with proposed revisions has been prepared. Coordination of the proposed changes and supplements began in October with the GCC, SCC, and PAG, to continue through January 2009 with the objective of completing the updated Annex for approval and publication by late March 2009.

IV. Cost Estimates – Implementation of the Public Transportation Security Strategy

TSA will provide appropriate cost estimates separately through the broader budgetary processes for DHS as coordinated by the Office of Management and Budget.

V. State of Public Transportation Security

The existing Mass Transit Annex to TS-SSP, produced in coordination with Transit, Commuter and Long Distance Rail GCC, Mass Transit SCC, and the Transit Policing and Security PAG, was published in June 2007. It presents the coordinated security enhancement strategy for public transportation and passenger rail systems. The Annex may be accessed at: http://www.tsa.gov/assets/pdf/modal_annex_mass_transit.pdf.

The information that follows provides an update on TSA’s efforts, in coordination with security partners in the Federal Government and mass transit and passenger rail mode, to

implement the security strategy and enhance its effectiveness.

TSA's efforts to assist public transit agencies and passenger rail carriers to deter terrorism and minimize the effects of terrorist attacks continue to be guided by five principles: (1) expanding partnerships for security enhancement through regional coordination and liaison, notably engagement with Federal and mass transit and passenger rail security partners through the GCC/SCC framework, the Transit Policing and Security PAG, and multi-agency coordination forums in regional areas throughout the country; (2) elevating the security baseline through the BASE program and the analysis and application of results to drive development of security programs and resource allocations that most effectively produce security enhancement; (3) building security force multipliers through security training of employees and law enforcement, terrorism prevention and response exercises and drills, and public awareness campaigns; (4) leading information assurance by building information sharing networks integrating Federal security partners with mass transit and passenger rail agencies and State and local entities to facilitate timely exchange of intelligence products and security implications at both classified and unclassified levels; and (5) protecting high risk assets and systems through development, testing, and deployment of new technologies and targeted application of security grants to achieve the most substantial mitigation of risk.

Expanding Partnerships for Security Enhancement

TSA is actively involved in regional security forums and supports these collaborative efforts through direct involvement of surface security inspectors and other liaison, timely sharing of intelligence products and related security information, and focused security initiatives. A key initiative of this effort is the joint classified threat and analysis briefings provided by intelligence professionals in DHS, TSA, and the FBI to mass transit and passenger rail security officials and their Federal partners. These sessions occur on at least a quarterly basis, with additional sessions as threat developments may warrant. They engage regional mass transit and passenger rail security professionals and their TSA and FBI colleagues in 15 metropolitan areas simultaneously through the FBI's secure video teleconference system maintained in the Joint Terrorism Task Force network.

TSA also helps facilitate Connecting Communities Emergency Response and Preparedness Forums to continue a successful TSA/FTA partnership project. The Connecting Communities program brings mass transit and passenger rail security partners together with regional first responders and Federal, State, and local government officials to discuss ways to enhance collaborative security prevention and emergency management response efforts. During 2007 and 2008, 13 Connecting Communities forums were held around the country. Eight have been scheduled already for 2009. These 2-day workshops enhance security and safety by sharing transit policies, procedures, resources, and best practices with local first responders to transit emergencies. The program uses realistic scenarios, including terrorism, to focus discussion on emergency preparedness, management, and response. A key objective is expanded understanding and effective integration of the roles of Federal, State, and local emergency management offices and response entities to facilitate efficient planning, preparedness, and response coordination.

TSA maintains extensive engagement with foreign counterparts on transit security matters with the aim of sharing and glean effective practices for potential integration in the domestic strategic approach. TSA conducts and maintains these efforts in collaboration and coordination with DHS component agencies, the Department of State, 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 the International Working Group on Land Transport Security (IWGLTS), a dedicated collaboration outside of any preexisting forum with primary focus on passenger rail and mass transit security. IWGLTS was formed to provide a global forum for experts to share best practices and lessons learned. The composition of the IWGLTS includes representatives from Australia, Canada, European Commission, France, Germany, India, Indonesia, Japan, Italy, Russia, Spain, United Kingdom, Republic of Korea, Malaysia, Israel, China, and the United States. TSA will chair this working group from mid-2008 through mid-2009, hosting a meeting in November 2008 in San Francisco and another yet to be scheduled in the first half of 2009. The group's efforts in 2007 led to several beneficial studies in mass transit and rail security, including in the areas of public awareness and recovery from an attack or incident involving chemical, biological, and radiological weapons and hazards.

TSA also maintains participation in the Rail and Urban Transport Working Group, consisting of the United States, United Kingdom, Canada, France, and Israel, in support of technology information sharing.

Elevating the Security Baseline

Under the BASE Program, TSA works with mass transit and passenger rail agencies to elevate their security posture. The BASE program assesses security posture in 17 Security and Emergency Management Action Items. Developed in a joint effort of TSA, DHS, DOT, and mass transit and passenger rail operating and security officials engaged through the Mass Transit SCC and Transit Policing and Security PAG, the Action Items encompass activities and measures that are foundational to an effective security program. Particular attention is paid to the transit agencies posture in six fundamental areas: protection of high-risk underwater/underground assets and systems; protection of other high-risk assets that have been identified through system-wide risk assessments; use of visible, unpredictable deterrence; targeted counter-terrorism training for key front-line staff; emergency preparedness drills and exercises; and public awareness and preparedness campaigns.

TSA's Transportation Security Inspectors (TSI) Surface conduct the assessments in partnership with the mass transit and passenger rail agencies' security chiefs and directors. The results of the security assessments inform development of risk mitigation

and security enhancement programs, resource allocations, and priorities for transit security grants.

Security assessments commenced during FY 2007 with an initial focus on the 50 largest mass transit and passenger rail agencies. In 2007, BASE assessments were conducted in 46 of the largest 50 transit agencies in the nation. To date, 88 BASE assessments have been completed in total, covering 48 of the largest 50 agencies, 30 ranked in the 51-100 range in size, and 10 smaller agencies. Three areas where assessments results produced timely action to address identified weaknesses were security training, random operational security activities, and drills and exercises. In response, TSA produced focused training guidance and revised and streamlined processes under the TSGP to expand training opportunities; coordinated approval for use of TSGP to fund dedicated anti-terrorism teams in high risk mass transit and passenger rail systems; and developed a national terrorism prevention exercise program for mass transit and passenger rail agencies and their regional security partners through the Intermodal Security Training and Exercise Program (I-STEP), meeting the mandate at Section 1407 of the 9/11 Act.

During the assessments, TSIs-Surface cite the most effective security programs, measures, and activities developed and implemented by mass transit and passenger rail agencies. This effort enabled production of a compilation of 55 Smart Security Practices, listed and summarized in six fundamental areas that align with TSA's strategic security priorities: Regional Partnerships and Information Sharing; Use of Random, Unpredictable Deterrence; Advancing the Security Baseline; Counterterrorism Training and Preparedness Exercises; Technology Applications to Mitigate High Consequence Risk; and Public Awareness and Preparedness Campaigns. TSA coordinated the preparation of this product with each agency with one or more practices cited, ensuring an accurate description of the practice and securing contact information for an official in the agency that professional colleagues may consult for more information. This compilation, a first in the transportation sector, fosters communication among security professionals in mass transit and passenger rail nationally with the specific objective of expanding adoption of these most effective practices, tailored as necessary to each agency's operating environment. TSA disseminated the Smart Security Practices compilation to law enforcement chiefs and security directors in mass transit and passenger rail in July 2008. As BASE assessments continue, this product will undergo periodic review, update, and expansion.

TSA surface inspectors are assigned to cover the key rail and mass transit facilities in more than 20 metropolitan areas around the country. Beyond conducting security assessments, inspectors serve as TSA's regional liaison to mass transit agencies and their local, State, and Federal security partners. During 2007, TSA surface inspectors conducted over 13,000 hours of stakeholder outreach, completed more than 1350 Station Profiles of passenger and transit rail stations, trained 139 Federal Security Directors (FSD)/FSD staff and Federal Air Marshal Service personnel in Railroad Operations Training in Pueblo, Colorado, and supported numerous Visible Intermodal Prevention and Response (VIPR) deployments nationwide.

TSA and its Federal partners continued their engagement with the American Public Transportation Association (APTA) Security Standards Policy and Planning Committee to develop security best practices to enhance security in transit systems. 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. TSA has provided subject matter expertise to the joint working groups, which cover three areas: infrastructure protection, emergency management, and risk assessment.

The proposed standards are being developed in a format that is consistent with American National Standards Institute 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 will be put forth as "recommended practices" and supported by APTA for voluntary adoption by the transit industry. TSA has provided the smart security practices derived from the BASE program security assessment results to the Mass Transit SCC for sharing with the appropriate working groups to spur progress and expedite completion of this lengthy effort.

Building Security Force Multipliers

Through the TSGP, DHS funds security enhancements in mass transit and passenger rail agencies in a risk-based approach. During FY 2009, the total allocation is \$348 million to eligible mass transit and passenger rail systems plus \$25 million to Amtrak. Total funding under the program in FY 2008 reached \$343 million plus \$25 million to Amtrak. In 2007, through the annual DHS appropriation and the supplemental, grant funding for transit security totaled \$255 million. Key priorities of the TSGP include protection of high risk assets and systems, including:

- Underwater tunnels and major terminals and stations;
- Targeted anti-terrorism training for employees;
- Terrorism prevention and response exercises and drills;
- Expanded public awareness campaigns; and
- Building in-house anti-terrorism capabilities through funding of a substantial portion of personnel, equipment, and training costs of dedicated operational teams.

Well-trained employees are a force multiplier for security efforts implemented by transit agencies in 2007. TSA developed and published the Mass Transit Security Training Program to assist transit agencies in improving security training of their employees. This program consists of guidelines for basic and follow-on training areas and specified subject areas in which particular categories of employees should receive training. It aligns with the components of a security training program Congress mandated under the 9/11 Act. TSA coordinated with DHS/FEMA, FTA, Mass Transit SCC, and the Transit Policing and Security Peer Advisory Group in developing these guidelines.

A focused initiative under the TSGP simplified the application process and facilitated more timely funding of training project requests. Course options include programs funded by FTA/TSA (transit specific terrorism prevention and response) and FEMA (general terrorism prevention and response). As such, these are integrated into National Training Program. Agencies taking advantage of this program in 2007 had their applications expedited for approval to ensure funds were delivered on a timelier basis than had been the case in the past. This initiative expanded significantly the volume and quality of training for transit employees. As an example, the proportion of grant awards for security training among eligible mass transit and passenger rail agencies in Tier 2 under the TSGP rose from 3 percent of the total funding allocation in FY 2006 to 68 percent in FY 2007.

During 2008, 441 VIPR deployments were conducted at various mass transit and passenger rail systems throughout the country as of the completion of this report. This scale of activity represents a marked increase over 2007, when 149 VIPR deployments occurred in mass transit and passenger rail. Deployed at the request of local officials, the TSA teams augment security in the systems and expand their capabilities to implement random, unpredictable security activities for deterrent effect. The varying force packages may consist of Federal Air Marshals, Behavior Detection Officers, TSIs, Transportation Security Officers, explosives detection canine teams, Explosives Security Specialists, and necessary supporting equipment. VIPR teams work with local security and law enforcement officials to supplement existing security resources, provide deterrent presence and detection capabilities, and introduce elements of randomness and unpredictability to disrupt potential terrorist planning activities.

To enhance coordination and deterrent effect, TSA and the representatives of the Transit Policing and Security PAG worked cooperatively and closely to improve coordination, preparation, planning, execution, and after action review of VIPR deployments in mass transit and passenger rail systems. This cooperation culminated with the completion of mutually agreed operating guidelines for "Effective Employment of Visible Intermodal Prevention and Response Teams in Mass Transit and Passenger Rail." The guidelines have been distributed to FSDs, Assistant Federal Security Directors-Surface, and Federal Air Marshal Special Agents-in-Charge around the country by the TSA Joint Coordination Center (JCC) to improve the effectiveness of the VIPR program. A follow-on product, developed and distributed in February 2008, details the roles and capabilities of the multiple TSA resources available to participate in VIPR deployments and provides recommendations on effective deployment in anti-terrorism activities.

To enhance terrorism prevention and immediate response capabilities, TSA is developing a national exercise program in partnership with mass transit and passenger rail agencies in the National Capital Region. Applying the Intermodal Security Training and Exercise Program (I-STEP) concept, TSA is advancing an exercise concept for nationwide distribution to facilitate planning, preparation, and execution of a multi-phased, multi-jurisdictional, and cross-functional anti-terrorism exercise program. The pilot effort in the Washington, DC, area included Amtrak, WMATA, Maryland Transit, and Virginia Railway Express, and other security partners. The initial coordination forum was held in

January 2008, with each of these agencies in attendance and agreeing to participate. Scenario-based anti-terrorism workshops followed over the next 3 months, with the principal agencies inviting their State and local security partners as additional participants. Coordination sessions held during May 2008 focused on preparing for the culminating event, a large scale regional table top exercise in Union Station, Washington, DC, on June 25, 2008.

Specific emphasis is placed on enhancing and testing prevention capabilities. TSA sponsored a second I-STEP exercise for mass transit and passenger and freight rail carriers and their regional security partners in northern New Jersey in late September 2008. Planning is ongoing to conduct similar exercises in the Los Angeles and Seattle areas during the first half of 2009.

Leading Information Assurance

TSA is advancing accomplishment of this strategic security priority through multiple means. A major initiative has been the interagency Mass Transit Security Information Network that ensures timely development and distribution to mass transit and passenger rail security officials and Federal government decision makers of security information products and recommendations and guidelines during periods of heightened threat or security incidents. The Homeland Security Information Network (HSIN) Public Transit Portal has been integrated into this network to provide a one-stop security information source and outlets for security advisories, alerts, and notices. To date, there has been 65 percent enrollment in HSIN-Public Transit portal among the 100 largest agencies, with 107 agencies enrolled in total. TSA expanded the target to integrate smaller agencies during FY 2008 and FY 2009. An ongoing effort with the Department's Office of Infrastructure Protection aims to advance a unified public/private information sharing environment that integrates alerts, warnings, and notifications; threat and suspicious activity or incident reporting; and effective data management and communications capabilities for enhanced collaboration during normal operations, security exercises, and responses to threats and incidents.

Joint DHS/TSA/FBI threat and analysis briefings at Secret level are held on a quarterly basis, bringing together mass transit and passenger rail security directors and law enforcement chiefs with their Federal security partners in 16 metropolitan areas through the secure video teleconferencing system maintained in the JTTF network. This capability enables timely assembly of these key officials through this means for unscheduled sessions as threats or security incidents warrant.

TSA has also aided in the deployment of secure telephone equipment to Amtrak and mass transit and passenger rail agencies ranked among the 20 largest to enable immediate contact to enable immediate exchange of intelligence on specific threats and other time-sensitive security concerns.

To increase the flow of information, TSA periodically disseminates Security Awareness Messages to mass transit and passenger rail security and management officials. Produced

generally on a monthly basis, these Messages provide DHS, FBI, and TSA intelligence products with security context and recommended use in training and awareness activities to mass transit and passenger rail agencies. During 2008, subjects addressed in these Messages have included a mass transit threat assessment; suicide bomber tradecraft and planning and point of attack indicators; next generation suicide bombers and use of elderly, female, and teenage operatives in terrorist attacks; second phase attacks to target first responders; analysis of future terrorist cells; a profile of Hezbollah; an overview of the security implications and recommended measures in light of hoax threat activity near the entrance to the Lincoln Tunnel in New Jersey; and situation reports and recommended security activities in light of the reported threat to New York City area transit systems and the terrorist attacks in Mumbai in late November 2008. With these Messages, TSA cites recommended protective measures and discusses use of the accompanying materials, which include intelligence products and training aids. Distribution occurs by direct e-mail using rosters for mass transit and passenger rail officials in 20 metropolitan areas and posting on HSIN-Public Transit portal.

Also in use is an Alert Notification System through which TSA maintains rosters of Federal security partners and security and management officials of mass transit and passenger rail agencies to ensure immediate notification of potential or actual threats and security incidents. Multiple address lists enable access to agencies based on size, geographic location, categories of officials, type of system, and nature of infrastructure.

Protecting High Risk Assets and Systems

Protecting high-risk underwater and underground assets and systems in mass transit is a top priority. The tunnel security working group formed by DHS and DOT continued to bring together subject matter experts from a range of relevant fields to identify, assess, and prioritize the risk to mass transit systems with underwater tunnels. The effort assists transit agencies in planning and implementing protective measures to deter and prevent attacks, and enhancing blast mitigation and emergency response capabilities. Through regular meetings, this effort has developed mitigation strategies, engaged security partners, analyzed and applied the results of risk assessments, prepared statements of work for testing and modeling programs, and integrated the overall risk mitigation effort for a cohesive, coordinated, and effective approach. Efforts to date have accomplished the following:

- Identified and assessed risk to underwater tunnels;
- Prioritized tunnel risk mitigation based on risk to drive DHS Transportation Security Grant Program funding to most pressing areas; and
- Produced and disseminated recommended protective measures transit agencies may implement to enhance security with available resources or through targeted grant funding.

The working group has developed strategies for funding for future technology research and development aimed at producing novel approaches to this challenging problem. For example, TSA is partnering with the DHS Science and Technology Directorate

(DHS/S&T) on a new program called "Resilient Tunnel." This program aims to address post-9/11 concerns that terrorists will target vulnerable tunnels causing catastrophic damages. Resilient Tunnel is a High Impact Technology Solutions project that is specifically pursuing novel solutions to protect critical transportation tunnels. The working group has also developed priorities for tunnel related transit security grant projects, such as expanded deployment of surveillance, monitoring, and detection technologies; anti-terrorism operational teams integrating dedicated law enforcement teams with explosives detection canine patrols for enhanced deterrence; and enhanced prevention and immediate response capabilities through anti-terrorism training, drills and exercises, and multi-media public awareness activities.

The National Explosives Detection Canine Team Program (NEDCTP) has continued to augment the explosives detection capability of critical transit agencies by providing partial funding, training, certification and management assistance. By the end of 2007, 62 TSA-certified explosives detection canine teams were deployed in a risk-based approach to 14 transit systems across the country. These teams provide a visible and effective detection and deterrence capability in the public transportation system and can be surged to other venues as threats dictate. Their mobility enables deployment randomly and unpredictably in patrols throughout passenger rail and mass transit systems and postings at key junctions or points within systems, stations, terminals, and facilities. The NEDCTP also established protocols for other agencies and departments to request the temporary use of TSA-certified canine teams during National Special Security Events and level 1 and 2 stolen explosive and recovery events.

Additionally, the TSGP guidance for FY 2007, and subsequent years, was revised to allow eligible agencies to procure the canines and training of the team through other sources that meet the TSA standard. Highly trained and certified canine teams continue to be one of the more effective and highly mobile explosives detection methods in the transit environment.

In coordination with DHS/S&T and TSA's Office of Security Technology, TSNM Mass Transit pursues development of multiple technologies to advance capabilities to detect and deter terrorist activity and prevent attacks. Project priorities are informed by input from security partners in the mass transit and passenger rail community. Particular priority is given to development of capabilities to mitigate the risk to underwater infrastructure. Ongoing development projects include:

- Anomalous Explosives Detector for Surface Transportation
- Intelligent Video Monitoring at Mass Transit Sites
- Bus Command and Control
- Chemical/Biological Program for Mass Transit
- Explosives Testing and Assessment of Rail Car Vulnerability
- Mass Transit Tunnels Entry Denial Systems
- Rapid Response to Extreme Events in Tunnels

**REPORT ON PROPOSED TRANSFER
THIRD QUARTER FISCAL YEAR (FY) 2008**

Operating Unit: Transportation Security Administration

**Fiscal Summary
(Dollars in Millions)**

Make Available To:		Amount
A. Checkpoint Support		\$2,152,991
Recovered /Deobligated From:		
A. Federal Flight Deck Officer	FY2007	\$ 5,666
B. Air Cargo	FY2007	\$ 29,954
C. Screener Partnership Program	FY2007	\$ 428,467
D. Screener Personnel, Compensation & Benefits	FY2007	\$1,136,440
E. Screener Training & Other	FY2007	\$ 218,443
F. Checkpoint Support	FY2007	\$ 86,004
G. Screening Technology, Maintenance and Utilities	FY2007	\$ 248,017

**Description/Justification
Total Increases: \$2,152,991**

Make Available To:

Aviation Appropriation

Checkpoint Support

<u>Current Plan</u>	<u>Increase</u>	<u>Revised Plan</u>
\$261,057,059	\$2,152,991	\$263,210,050

(Includes carryover of \$2.6M, \$250M in the Aviation Checkpoint Security Fund, and \$8.4M Reprogram)

As provided in Section 521 of the FY 2008 Department of Homeland Security Appropriations Act (P.L. 110-161), TSA will use \$2,152,991 for the Checkpoint Support Program for procurement and installation of explosive detection technology. The additional funding will be used to accelerate deployment of equipment and sensors within the Checkpoint Support Program to detect an increased range of threats.

Effects on Pending or Future Appropriations

This action for FY 2008 is intended to provide the necessary funding to accelerate initiatives of the Checkpoint Support Program. There is no immediate effect on pending appropriations as the strategy to transform the checkpoint technology covers multiple fiscal years and immediate equipment purchases will be under warranty. Future years' budget requests will reflect the impacts to the overall Checkpoint Strategic Plan.

Impact on Departmental or Congressional Policies

This action would not require a shift in the Department of Homeland Security, Office of Management and Budget, or Congressionally approved objectives and policies.

**Recovery/Deobligation from
Total Decreases: \$2,152,991**

Recovered Deobligated From: Prior year recoveries in the Aviation Security Appropriation.

Effects on Pending or Future Appropriations

This action will not impact pending or future appropriations. It is a one time adjustment of recoveries per the General Provision. The recoveries were obtained by de-obligating funds on contracts where the period of performance was expired. No planned activities in these programs will be affected.

Impact on Departmental or Congressional Policies

This action would not require a shift in the Department of Homeland Security, Office of Management and Budget, or Congressionally approved objectives and policies.

**REPORT ON PROPOSED TRANSFER
FISCAL YEAR (FY) 2008**

Operating Unit: Transportation Security Administration

**Fiscal Summary
(Dollars in Millions)**

Make Available To:	Amount
EDS/ETD Procurement and Installation PPA	\$65,000,000*
Checkpoint Support PPA	\$17,700,000

*Of this amount, \$50 million is included in the existing EDS Spend Plan. Allocation of the remaining \$15 million is pending quarterly review of the spend plan. An update will be provided.

**Description/Justification
Total Increase: \$82,700,000**

Recovered/Deobligated From:		Amount
Privatized Screening	FY 2005	10,000,000
Screening Training and Other	FY 2005	1,650,000
Human Resource Services	FY 2005	3,000,000
Screening Technology Maintenance and Utilities	FY 2005	22,000,000
Checkpoint Support	FY 2005	18,000,000
Airport Management, IT and Support	FY 2005	8,000,000
Aviation Regulation and Other Enforcement	FY 2004/2005	12,000,000
FFDO and Flight Crew Training	FY 2004/2005	2,350,000
Air Cargo	FY 2004/2005	1,700,000
Secure Flight (CAPPS II)	FY 2004	4,000,000
Total		82,700,000

Aviation Appropriation

**EDS/ETD Procurement and Installation PPA
Checkpoint Support PPA**

<u>Current Plan</u>	<u>Increase</u>	<u>Revised Plan</u>
EDS \$294,000,000	\$65,000,000	\$359,000,000
PSP \$250,000,000	\$17,700,000	\$267,700,000

As provided in Section 521 of the FY 2008 Department of Homeland Security Appropriations Act (P.L. 110-161), TSA will use \$65,000,000 for the EDS/ETD Procurement and Installation PPA and \$17,700,000 for the Checkpoint PPA. The additional funding for EDS will be used to fund Other Transaction Agreements (OTA) with Los Angeles International Airport and San Jose International Airport. Funding for Checkpoint will be used for the purchase and installation of equipment to detect an increased range of threats.

Effects on Pending or Future Appropriations

This action for FY 2009 is intended to provide the necessary funding for initiatives in the EDS/ETD Procurement and Installation and Checkpoint Support Programs. There will be no immediate effect on pending appropriations as the strategies to transform the checkpoint and deploy optimal in-line EDS for baggage systems covers multiple years.

Impact on Departmental or Congressional Policies

This action would not require a shift in the Department of Homeland Security, Office of Management and Budget, or Congressionally approved objectives and policies.

**Recovery/Deobligation from
Total Decreases: \$82,700,000**

Recovered Deobligated From: Prior year recoveries in the Aviation Security Appropriation.

Effects on Pending or Future Appropriations

This action will not impact pending or future appropriations. It is a one time adjustment of recoveries per the General Provision. The recoveries were obtained by deobligating funds on contracts where the period of performance was expired. No planned activities in these programs will be affected.

Impact on Departmental or Congressional Policies

This action would not require a shift in the Department of Homeland Security, Office of Management and Budget, or Congressionally approved objectives and policies.

FOR OFFICIAL USE ONLY



Passenger Screening Wait Times

Fiscal Year 2009 Report to Congress

1st Quarter

April 13, 2009



Homeland
Security

Transportation Security Administration

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Message from the Acting Administrator

April 13, 2009

I am pleased to present the following report, "Passenger Screening Wait Times," which has been prepared by the Transportation Security Administration (TSA).

This document has been prepared pursuant to a requirement in the Fiscal Year (FY) 2009 Department of Homeland Security Appropriations Act (P.L. 110-329), which directs TSA to submit airport wait time data on a quarterly basis for domestic airports with above average wait times and for the 40 busiest (Focus 40) airports. The following report provides passenger screening wait times for the first quarter of FY 2009.

Pursuant to congressional requirements, this report is being provided to the following Members of Congress:

The Honorable David E. Price
Chairman, House Appropriations Subcommittee on Homeland Security

The Honorable Harold Rogers
Ranking Member, House Appropriations Subcommittee on Homeland Security

The Honorable Robert Byrd
Chairman, Senate Appropriations Subcommittee on Homeland Security

The Honorable George V. Voinovich
Ranking Member, Senate Appropriations Subcommittee on Homeland Security

Inquiries relating to this report may be directed to me at (571) 227-2801 or to the Department's Acting Chief Financial Officer, Peggy Sherry, at (202) 447-5751.

Sincerely,



Gale Rossides
Acting Administrator
Transportation Security Administration

Executive Summary

The FY 2009 Department of Homeland Security Appropriations Act (P.L. 110-329) directs TSA to report to Congress passenger screening wait time data on a quarterly basis for domestic airports with above average wait times and for the 40 busiest (Focus 40) airports.

TSA compared passenger screening wait times for the first quarters of FY 2008 and FY 2009. The data shows that at airports nationwide, 99.6 percent of passengers experienced wait times of less than 20 minutes, an increase of 3.8 percent from the 95.8 percent of passengers who experienced wait times of less than 20 minutes in the first quarter of FY 2008.

At the Focus 40 airports, the results were very similar: 99.5 percent of passengers experienced wait times of less than 20 minutes, an increase of 4.8 percent from the 94.7 percent of passengers who experienced wait times of less than 20 minutes in the first quarter of FY 2008. The data also provides an explanation of significant changes in wait times at three airports.

TSA continues to maintain a 10-minute wait time standard.



Passenger Screening Wait Times
1st Quarter, Fiscal Year 2009

Table of Contents

I. Legislative Requirement	1
II. Background	1
III. Passenger Screening Wait Time Data	2
IV. Performance Highlights and Major Change Notes	3
V. Conclusion	4
VI. Appendix: Glossary of Terms	4

FOR OFFICIAL USE ONLY

I. Legislative Requirement

The Fiscal Year (FY) 2009 Department of Homeland Security Appropriations Act (P.L. 110-329) states:

Consistent with prior years, TSA shall continue to submit airport wait time data on a quarterly basis for domestic airports with above average wait times and for the top 40 busiest airports. As part of these reports, TSA shall explain any dramatic shift in wait times and what is being done to reduce wait times at these airports. TSA shall not alter its current 10 minute standard.

This report has been compiled in response to that requirement.

II. Background

The Transportation Security Administration (TSA) collects throughput (the number of persons screened) data through counters located at the walk-through metal detector (WTMD) or whole-body imager (WBI) at the entrance to each screening lane within a checkpoint. Since 2004, TSA has reduced average wait times nationwide to less than 5 minutes through checkpoint process optimization and continuous improvement initiatives. Since September 11, 2008, TSA has focused on reducing passenger wait time incidents of 20 minutes or more. These incidents are reported along with the hourly throughput counts to each airport coordination center, which uploads the data to TSA's Performance Management Information System (PMIS) on a daily basis. The wait time data contained in this report was generated from PMIS and compares wait time performance in the first quarter of FY 2009 to wait time data for the first quarter of FY 2008. The throughput information provides insight as to passenger travel demand and seasonality changes.

FOR OFFICIAL USE ONLY

III. Passenger Screening Wait Time Data

9/30/07-1/05/08 vs 9/27/06-1/03/08 Wait Time and Throughput Comparison

Source: TSA PIMS BI Tool as of January 8, 2009

Airport	Quarter 1 FY09				Quarter 1 FY08				Throughput Absolute Change (FY09-FY08)	Relative Change (FY09 - FY08)		
	Total Throughput	% Passengers Waiting < 20 Minutes	% Passengers Waiting 20-30 Minutes	% Passengers Waiting > 30 Minutes	Total Throughput	% Passengers Waiting < 20 Minutes	% Passengers Waiting 20-30 Minutes	% Passengers Waiting > 30 Minutes		% Passengers Waiting < 20 Minutes	% Passengers Waiting 20-30 Minutes	% Passengers Waiting > 30 Minutes
TSA Nationwide	165,957,699	99.6%	0.4%	0.0%	187,521,784	95.8%	3.7%	0.5%	-11.5%	3.8%	-3.3%	-0.5%
F-40 Focus 40 Airports	120,832,998	99.5%	0.4%	0.0%	135,302,969	94.7%	4.6%	0.7%	-10.7%	4.8%	-4.2%	-0.6%
ATL Hartsfield Atlanta International Airport	5,080,993	100%	0.0%	0.0%	5,433,373	84.1%	12%	3%	-6.5%	15.9%	-12.5%	-3.4%
BOS Logan International Airport	3,900,206	99.6%	0.3%	0.0%	4,237,585	98.7%	1.1%	0.2%	-8.0%	0.9%	-0.7%	-0.2%
BWI Baltimore-Washington Int'l Airport	2,385,348	100.0%	0.0%	0.0%	2,595,849	99.7%	0.3%	0.0%	-8.1%	0.3%	-0.3%	0.0%
CLE Cleveland Hopkins International Airport	1,101,376	99.8%	0.2%	0.0%	1,286,267	96.6%	2.7%	0.7%	-14.4%	3.2%	-2.5%	-0.7%
CLT Charlotte/Douglas International Airport	1,635,968	100.0%	0.0%	0.0%	1,794,006	93.9%	5.6%	0.4%	-8.8%	6.0%	-5.6%	-0.4%
CVG Cincinnati/Northern Kentucky Int'l Airport	625,493	99.7%	0.3%	0.0%	732,562	98.1%	1.7%	0.2%	-14.6%	1.6%	-1.4%	-0.2%
DCA Ronald Reagan Washington National Airpo	2,157,205	99.7%	0.3%	0.0%	2,238,510	99.4%	0.6%	0.0%	-3.6%	0.3%	-0.3%	0.0%
DEN Denver International Airport	3,628,854	99.2%	0.7%	0.1%	3,920,919	95.8%	3.8%	0.3%	-7.4%	3.4%	-3.1%	-0.3%
DFW Dallas/Fort Worth International Airport	5,551,709	100.0%	0.0%	0.0%	5,894,033	94.8%	4.6%	0.6%	-5.8%	5.2%	-4.6%	-0.6%
DTW Detroit Metro Wayne County Airport	2,672,378	100.0%	0.0%	0.0%	2,959,058	99.1%	0.8%	0.1%	-9.7%	0.9%	-0.8%	0.0%
EWB Newark International Airport	4,566,409	99.0%	0.9%	0.1%	5,058,612	96.0%	3.2%	0.8%	-9.7%	3.0%	-2.3%	-0.7%
FLL Ft Lauderdale-Hollywood Int'l Airport	2,794,098	99.9%	0.1%	0.0%	3,326,432	93.9%	5.7%	0.4%	-16.0%	6.0%	-5.7%	-0.4%
HNL Honolulu International Airport	1,873,808	100.0%	0.0%	0.0%	2,290,002	99.7%	0.3%	0.0%	-18.2%	0.3%	-0.3%	0.0%
IAD Washington-Dulles Int'l Airport	2,429,143	100.0%	0.0%	0.0%	2,648,959	89.6%	8.2%	2.2%	-8.3%	10.4%	-8.2%	-2.2%
IAH George Bush Intercontinental Airport Hous	3,396,770	100.0%	0.0%	0.0%	3,726,150	99.5%	0.5%	0.0%	-8.8%	0.5%	-0.4%	0.0%
IND Indianapolis International Airport	1,147,423	99.7%	0.3%	0.0%	1,258,523	99.8%	0.2%	0.0%	-8.8%	-0.1%	0.1%	0.0%
JFK John F. Kennedy International Airport	6,511,679	99.7%	0.3%	0.0%	6,835,864	95.7%	4.1%	0.2%	-4.7%	4.0%	-3.8%	-0.2%
LAS McCarran International Airport	4,783,194	100.0%	0.0%	0.0%	5,496,125	84.5%	11.2%	4.3%	-13.0%	15.5%	-11.2%	-4.3%
LAX Los Angeles International Airport	8,277,829	98.0%	1.8%	0.2%	9,093,006	97.3%	2.6%	0.1%	-9.0%	0.7%	-0.8%	0.1%
LGA LaGuardia Airport	3,299,862	98.3%	1.4%	0.3%	4,014,915	96.9%	2.6%	0.5%	-17.8%	1.4%	-1.2%	-0.2%
MCI Kansas City International Airport	1,885,801	99.9%	0.1%	0.0%	1,948,694	99.9%	0.1%	0.0%	-3.2%	-0.1%	0.1%	0.0%
MCO Orlando International Airport	4,565,791	100.0%	0.0%	0.0%	5,958,217	96.9%	2.8%	0.3%	-23.4%	3.1%	-2.8%	-0.3%
MDW Chicago Midway Airport	1,694,039	100.0%	0.0%	0.0%	2,018,870	98.2%	1.8%	0.0%	-16.1%	1.8%	-1.8%	0.0%
MIA Miami International Airport	4,093,721	99.7%	0.3%	0.0%	4,165,708	81.6%	17.6%	0.8%	-1.7%	18.1%	-17.4%	-0.8%
MSP Minneapolis-St. Paul International Arpt	2,559,241	100.0%	0.0%	0.0%	3,009,945	95.6%	4.1%	0.4%	-15.0%	4.4%	-4.1%	-0.4%
OAK Oakland International Airport	1,547,797	99.7%	0.3%	0.0%	2,152,598	96.3%	3.5%	0.2%	-28.1%	3.4%	-3.2%	-0.2%
ORD O'Hare International Airport	6,037,150	98.9%	1.1%	0.0%	6,882,742	94.4%	5.3%	0.3%	-12.3%	4.5%	-4.3%	-0.2%
PDX Portland International	1,719,723	99.8%	0.2%	0.0%	1,936,162	99.4%	0.6%	0.0%	-11.2%	0.4%	-0.4%	0.0%
PHL Philadelphia International Airport	3,305,986	98.5%	1.5%	0.0%	3,600,146	90.3%	9.1%	0.6%	-8.2%	8.2%	-7.6%	-0.6%
PHX Phoenix Sky Harbor International Airport	3,910,853	99.0%	1.0%	0.1%	4,542,902	93.1%	6.0%	0.9%	-13.9%	5.8%	-5.1%	-0.8%
RDU Raleigh-Durham International Airport	1,357,735	99.9%	0.1%	0.0%	1,436,013	97.8%	2.1%	0.1%	-5.5%	2.1%	-2.0%	-0.1%
SAN San Diego International Airport, Lindbergh	2,373,923	98.8%	0.9%	0.2%	2,585,223	92.3%	7.2%	0.5%	-8.2%	6.6%	-6.3%	-0.3%
SEA Seattle-Tacoma Int'l Airport	3,437,084	99.0%	0.7%	0.3%	3,723,358	92.5%	6.7%	0.7%	-7.7%	6.5%	-6.0%	-0.5%
SFO San Francisco Int'l Airport	5,050,599	99.9%	0.1%	0.0%	5,121,273	99.5%	0.4%	0.0%	-1.4%	0.4%	-0.4%	0.0%
SJU Luis Munoz Marin Int'l Airport	1,067,975	99.9%	0.1%	0.0%	1,286,577	91.9%	6.3%	1.8%	-17.0%	8.0%	-6.2%	-1.8%
SLC Salt Lake City Int'l Airport	1,530,099	99.7%	0.3%	0.0%	1,675,613	94.9%	4.9%	0.2%	-8.7%	4.8%	-4.6%	-0.2%
SMF Sacramento International Airport	1,460,981	100.0%	0.0%	0.0%	1,687,218	96.2%	3.6%	0.1%	-13.4%	3.8%	-3.6%	-0.1%
SNA John Wayne Airport	1,120,820	100.0%	0.0%	0.0%	1,524,156	94.8%	4.6%	0.6%	-26.5%	5.2%	-4.6%	-0.6%
STL Lambert St Louis International Airport	1,788,236	100.0%	0.0%	0.0%	1,942,255	96.4%	3.1%	0.5%	-7.9%	3.6%	-3.1%	-0.5%
TPA Tampa International Airport	2,505,699	100.0%	0.0%	0.0%	3,264,549	95.3%	4.6%	0.2%	-23.2%	4.7%	-4.6%	-0.2%

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

IV. Performance Highlights and Major Change Notes

Focus Airport	Focus Airport Name	Quarter 1 FY09				Relative Change (FY09 - FY08)			
		Total Throughput	% Passengers Waiting < 20 Minutes	% Passengers Waiting 20-30 Minutes	% Passengers Waiting > 30 Minutes	Total Throughput	% Passengers Waiting < 20 Minutes	% Passengers Waiting 20-30 Minutes	% Passengers Waiting > 30 Minutes
MIA	Miami International Airport	4,093,721	99.7%	0.3%	0.0%	-1.7%	18.1%	-17.4%	-0.8%
						-71,987 decreased	Improvement In Wait	Improvement In Wait	Improvement In Wait

Change: New FSD was appointed at MIA between the 4th Quarter FY07 and 4th Quarter FY08.

MIA achieved 99.7% of its passengers waiting less than 20 minutes - an improvement of 18.1%. Throughput decreased by -1.7%.

Reasons for [relative] significant change:

Processing capacity improved

- Total redesign of all checkpoints: Added 2-sided queue at Transport Document Checking (TDC), using 2 X-rays served by 1 Walk-Thru Metal Detector (a.k.a. 2:1 layout), optimizing divest and recompose roller lengths.
- Staffing changed to allocate Part Time and Split Shift TSO's during peak periods
- Local hiring (improved process allows TSA to quickly add and backfill new employees).

Focus Airport	Focus Airport Name	Quarter 1 FY09				Relative Change (FY09 - FY08)			
		Total Throughput	% Passengers Waiting < 20 Minutes	% Passengers Waiting 20-30 Minutes	% Passengers Waiting > 30 Minutes	Total Throughput	% Passengers Waiting < 20 Minutes	% Passengers Waiting 20-30 Minutes	% Passengers Waiting > 30 Minutes
ATL	Hartsfield Atlanta International Airport	5,080,993	100.0%	0.0%	0.0%	-6.5%	15.9%	-12.5%	-3.4%
						-352,380 decreased	Improvement In Wait	Improvement In Wait	Improvement In Wait

Change: ATL experienced a major change in operating leadership during 2008. Significant outside resources (optimization teams, experienced managers/coaches) were deployed 4-9/08 to improve all aspects of screening operations.

ATL achieved 100.0% of its passengers waiting less than 20 minutes - an improvement of 15.9%. Throughput decreased by -6.5%.

Reasons for [relative] significant change:

Passenger and business growth

- Reorganization of staffing - reduction of TSOs assigned to baggage and an increase in TSOs assigned to checkpoints
- Improved scheduling including shift bids on six month timetable, instead of annual. This increases flexibility to adjust schedules to operational and officer needs
- Improved infrastructure including: addition of 5 additional lanes, redesigned queues, integrated selectee lanes, and self select lanes

Focus Airport	Focus Airport Name	Quarter 1 FY09				Relative Change (FY09 - FY08)			
		Total Throughput	% Passengers Waiting < 20 Minutes	% Passengers Waiting 20-30 Minutes	% Passengers Waiting > 30 Minutes	Total Throughput	% Passengers Waiting < 20 Minutes	% Passengers Waiting 20-30 Minutes	% Passengers Waiting > 30 Minutes
LAS	McCarran International Airport	4,783,194	100.0%	0.0%	0.0%	-13.0%	15.5%	-11.2%	-4.3%
						-712,931 decreased	Improvement In Wait	Improvement In Wait	Improvement In Wait

Change: LAS experienced a decrease of over 712K passengers from previous Oct - Dec period due significantly to the world-wide economic slowdown

LAS achieved 100.0% of its passengers waiting less than 20 minutes - an improvement of 15.5%. Throughput decreased by -13.0%

Reasons for [relative] significant change:

Processing capacity improved

- TSA Checkpoint reconfiguration to 2:1 layout; which uses 1 walk-through metal detector (WTMD) to feed passengers to 2 X-rays - the need for another officers manning the 2nd WTMD.
- Increased part-time/full-time TSO ratios to appropriately staff peaks with part-time staff.
- Demand-based schedule vs. rotation schedule; i.e., lunch, breaks, and training times are done before or after peak periods, not during peaks.
- Local hiring (improved process allows TSA to quickly fill vacancies).

Notes: * The Change formula for throughput is $[(FY08-FY07)/FY07]$; while the changes in percentage thresholds of 20 and 30 minutes are $[(FY08\% - FY07\%)]$.

TSA has modified the measure of wait from high-labor burden in sampling actual times to counting wait time events exceeding 20 and 30 minutes.

This change focuses the workforce on security, since over 99% of passengers are being screened with wait times of less than 20 minutes (an improvement from 97% in FY07).

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

V. Conclusion

In conclusion, industry passenger travel in the first quarter of fiscal year 2009 has declined 11 percent from the previous year, as measured by the checkpoint throughput (count of persons screened). Nationwide, TSA continues to be significantly below the average wait time standard of 10 minutes. Incidents of passenger wait times of 20 minutes or more was reduced by more than 4 percent in the Focus 40 airports.

VII. Appendix: Glossary of Terms

2:1 Layout	Two X-ray served by one WTMD – reduces one Transportation Security Officer fixed position among other efficiency improvements at security checkpoints
9/11 Act	Implementing Recommendations of the 9/11 Commission Act (P. L. 110-53)
DHS	Department of Homeland Security
FLETC	Federal Law Enforcement Training Center
Focus 40	Set of forty airports which represent the largest U.S. Airports under the Transportation Security Administration
FY	Fiscal Year
OMB	Office of Management and Budget
SAM	Staffing Allocation Model used by TSA to forecast passenger security screening demand, allocate and schedule TSO's
Throughput	Security screening demand which includes passengers, airline industry workers. In the context of checked baggage, it is the number of checked bags and packages screened by TSA
TIP	Threat Image Projection program that overlays threat images on to X-ray images continually testing TSO threat detection capabilities
TRX	TIP-Ready X-ray at a passenger security checkpoint
TSA	Transportation Security Administration
TSO	Transportation Security Officer
WBI	Whole-Body Imager detects possible threats on persons at security checkpoints
WTMD	Walk-through Metal Detection machine at the security checkpoint



Passenger Screening Wait Times

Fiscal Year 2009 Report to Congress

Second Quarter

July 13, 2009



Homeland
Security

Transportation Security Administration

Message from the Acting Administrator

July 13, 2009

I am pleased to present the following report, "Passenger Screening Wait Times," which has been prepared by the Transportation Security Administration in response to a requirement accompanying the Fiscal Year (FY) 2009 Department of Homeland Security Appropriations Act (P.L. 110-329). This report provides 2nd quarter FY 2009 airport wait time data for domestic airports with above average wait times and for the 40 busiest (Focus 40) airports.

Pursuant to congressional requirements, this report is being provided to the following:

The Honorable David E. Price
Chairman, House Appropriations Subcommittee on Homeland Security

The Honorable Harold Rogers
Ranking Member, House Appropriations Subcommittee on Homeland Security

The Honorable Robert C. Byrd
Chairman, Senate Appropriations Subcommittee on Homeland Security

The Honorable George V. Voinovich
Ranking Member, Senate Appropriations Subcommittee on Homeland Security

The Honorable James L. Oberstar
Chairman, House Committee on Transportation and Infrastructure

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

The Honorable John D. Rockefeller, IV
Chairman, Senate Committee on Commerce, Science, and Transportation

The Honorable Kay Bailey Hutchison
Ranking Member, Senate Committee on Commerce, Science, and Transportation

If I may be of further assistance, please do not hesitate to contact me at (571) 227-2845 or the Department's Acting Chief Financial Officer, Peggy Sherry, at (202) 447-5751.

Sincerely yours,



Gale D. Rossides
Acting Administrator

Executive Summary

The Fiscal Year (FY) 2009 Department of Homeland Security Appropriations Act directs the Transportation Security Administration (TSA) to report to Congress passenger screening wait time data on a quarterly basis for domestic airports with above average wait times and for the 40 busiest (Focus 40) airports.

TSA compared passenger screening wait times for the second quarters of FY 2008 and FY 2009. The data shows that at airports nationwide, 99.7 percent of passengers experienced wait times of less than 20 minutes, an increase of 3.5 percent from the 96.2 percent of passengers who experienced wait times of less than 20 minutes in the second quarter of FY 2008.

At the Focus 40 airports, the results were very similar: 99.7 percent of passengers experienced wait times of less than 20 minutes, an increase of 4.2 percent from the 95.4 percent of passengers who experienced wait times of less than 20 minutes in the second quarter of FY 2008. The data also provides an explanation of significant changes in wait times at three airports.

TSA continues to maintain a 10-minute wait time standard.



Passenger Screening Wait Times Fiscal Year 2009, 2nd Quarter

Table of Contents

I. Legislative Requirement	1
II. Background	1
III. Passenger Screening Wait Time Data	2
IV. Performance Highlights and Major Change Notes	3
V. Conclusion	4
VI. Appendix A: Glossary of Terms	5

I. Legislative Requirement

The Fiscal Year 2009 Department of Homeland Security Appropriations Act (P.L. 110-329) states:

Consistent with prior years, TSA shall continue to submit airport wait time data on a quarterly basis for domestic airports with above average wait times and for the top 40 busiest airports. As part of these reports, TSA shall explain any dramatic shift in wait times and what is being done to reduce wait times at these airports. TSA shall not alter its current 10-minute standard.

This report is submitted in accordance with that requirement.

II. Background

TSA collects throughput (the number of persons screened) data through counters located at the walk-through metal detector (WTMD) or whole-body imager (WBI) at the entrance to each screening lane within a checkpoint. Since 2004, TSA has reduced average wait times nationwide to less than 5 minutes through checkpoint process optimization and other continuous improvement initiatives. Since September 11, 2008, TSA has focused on reducing passenger wait time incidents of 20 minutes or more. These incidents are reported along with the hourly throughput counts to each airport coordination center, which uploads the data to TSA's Performance Management Information System (PMIS) on a daily basis. The wait time data contained in this report was generated from PMIS and compares wait time performance in the second quarter of FY 2009 to wait time data for the second quarter of FY 2008. The throughput information provides insight as to passenger travel demand and seasonality changes.

Airport		Quarter 2 FY09				Quarter 2 FY08				Relative Change (FY09 - FY08)			
		Customer Throughput - Chpt, Date, Hr				Customer Throughput - Chpt, Date, Hr				Throughput Absolute Change (FY09-FY08) /FY08			
		Total Throughput	% Passengers Waiting < 20 Minutes	% Passengers Waiting 20-30 Minutes	% Passengers Waiting > 30 Minutes	Total Throughput	% Passengers Waiting < 20 Minutes	% Passengers Waiting 20-30 Minutes	% Passengers Waiting > 30 Minutes		% Passengers Waiting < 20 Minutes	% Passengers Waiting 20-30 Minutes	% Passengers Waiting > 30 Minutes
TSA	Nationwide	134,002,029	99.7%	0.3%	0.0%	156,551,039	96.2%	3.4%	0.4%	-14.4%	3.5%	-3.1%	-0.3%
F-40	Focus 40 Airports	96,990,538	99.7%	0.3%	0.0%	112,388,977	95.4%	4.1%	0.5%	-13.7%	4.2%	-3.8%	-0.4%
ATL	Hartsfield Atlanta International Airport	3,945,462	100.0%	0.0%	0.0%	4,591,763	81.7%	14.4%	3.9%	-14.1%	18.3%	-14.4%	-3.9%
BOS	Logan International Airport	3,022,012	99.9%	0.0%	0.1%	3,225,421	98.6%	1.3%	0.1%	-6.3%	1.3%	-1.3%	0.0%
BWI	Baltimore-Washington Int'l Airport	1,861,732	100.0%	0.0%	0.0%	2,015,183	99.9%	0.0%	0.1%	-7.6%	0.1%	0.0%	-0.1%
CLE	Cleveland Hopkins International Airport	863,484	100.0%	0.0%	0.0%	1,055,733	98.0%	1.9%	0.1%	-18.2%	2.0%	-1.9%	-0.1%
CLT	Charlotte/Douglas International Airport	1,298,859	100.0%	0.0%	0.0%	1,476,825	94.8%	4.9%	0.3%	-12.1%	5.2%	-4.9%	-0.3%
CVG	Cincinnati/Northern Kentucky Intl. AP	497,835	99.5%	0.5%	0.0%	613,173	99.0%	1.0%	0.0%	-18.8%	0.6%	-0.6%	0.0%
DCA	Ronald Reagan Washington National AP	1,724,315	99.4%	0.2%	0.3%	1,745,759	99.8%	0.2%	0.0%	-1.2%	-0.3%	0.0%	0.3%
DEN	Denver International Airport	3,033,207	98.7%	1.2%	0.1%	3,394,966	97.1%	2.5%	0.4%	-10.7%	1.6%	-1.3%	-0.3%
DFW	Dallas/Fort Worth International Airport	4,306,434	100.0%	0.0%	0.0%	4,810,540	97.7%	2.3%	0.0%	-10.5%	2.3%	-2.3%	0.0%
DTW	Detroit Metro Wayne County Airport	2,069,056	100.0%	0.0%	0.0%	2,628,227	98.9%	0.9%	0.2%	-21.3%	1.1%	-0.9%	-0.2%
EWB	Newark International Airport	3,466,560	99.5%	0.4%	0.0%	4,106,369	98.4%	1.2%	0.3%	-15.6%	1.1%	-0.8%	-0.3%
FLL	Ft Lauderdale-Hollywood Intl Arpt	2,716,192	99.8%	0.1%	0.0%	3,163,209	96.3%	3.6%	0.1%	-14.1%	3.5%	-3.4%	-0.1%
HNL	Honolulu International Airport	1,654,015	100.0%	0.0%	0.0%	1,921,993	99.8%	0.2%	0.0%	-13.9%	0.2%	-0.2%	0.0%
IAD	Washington-Dulles Intl Airport	1,886,195	99.9%	0.1%	0.0%	2,097,939	94.7%	4.5%	0.9%	-10.1%	5.2%	-4.4%	-0.9%
IAH	George Bush Intercont'l Airport Houston	2,708,668	100.0%	0.0%	0.0%	3,183,051	99.8%	0.2%	0.0%	-14.9%	0.2%	-0.2%	0.0%
IND	Indianapolis International Airport	907,410	100.0%	0.0%	0.0%	1,008,483	99.1%	0.7%	0.2%	-10.0%	0.9%	-0.7%	-0.2%
JFK	John F. Kennedy International Airport	4,917,156	100.0%	0.0%	0.0%	5,385,476	97.2%	2.6%	0.1%	-8.7%	2.7%	-2.6%	-0.1%
LAS	McCarran International Airport	4,042,817	99.9%	0.1%	0.0%	4,621,906	89.4%	9.5%	1.2%	-12.5%	10.5%	-9.3%	-1.2%
LAX	Los Angeles International Airport	6,443,775	98.4%	1.4%	0.1%	7,409,787	98.0%	1.9%	0.2%	-13.0%	0.5%	-0.4%	0.0%
LGA	LaGuardia Airport	2,416,128	99.4%	0.6%	0.0%	2,907,030	97.2%	2.6%	0.2%	-16.9%	2.1%	-2.0%	-0.2%
MCI	Kansas City International Airport	1,415,085	100.0%	0.0%	0.0%	1,529,217	99.9%	0.1%	0.0%	-7.5%	0.1%	-0.1%	0.0%
MCO	Orlando International Airport	4,123,007	100.0%	0.0%	0.0%	5,376,663	89.7%	9.3%	1.0%	-23.3%	10.3%	-9.3%	-1.0%
MDW	Chicago Midway Airport	1,305,569	98.8%	1.2%	0.0%	1,504,495	98.5%	1.5%	0.0%	-13.2%	0.2%	-0.2%	0.0%
MIA	Miami International Airport	3,619,225	99.9%	0.1%	0.0%	3,801,434	82.3%	17.2%	0.5%	-4.8%	17.6%	-17.1%	-0.5%
MSP	Minneapolis-St. Paul International Arpt	2,393,921	100.0%	0.0%	0.0%	2,753,901	99.4%	0.6%	0.0%	-13.1%	0.6%	-0.6%	0.0%
OAK	Oakland International Airport	1,120,459	100.0%	0.0%	0.0%	1,592,913	96.1%	3.7%	0.1%	-29.7%	3.9%	-3.7%	-0.1%
ORD	O'Hare International Airport	4,521,993	99.6%	0.3%	0.0%	5,482,619	98.0%	2.0%	0.0%	-17.5%	1.6%	-1.7%	0.0%
PDX	Portland International	1,303,758	100.0%	0.0%	0.0%	1,511,311	99.9%	0.1%	0.0%	-13.7%	0.1%	-0.1%	0.0%
PHL	Philadelphia International Airport	2,508,888	99.9%	0.1%	0.0%	2,989,828	92.9%	6.8%	0.3%	-16.1%	7.1%	-6.8%	-0.3%
PHX	Phoenix Sky Harbor International Airport	3,437,622	99.1%	0.9%	0.0%	4,048,361	92.3%	6.9%	0.9%	-15.1%	6.8%	-6.0%	-0.8%
RDU	Raleigh-Durham International Airport	973,125	100.0%	0.0%	0.0%	1,120,675	96.6%	3.3%	0.2%	-13.2%	3.4%	-3.3%	-0.2%
SAN	San Diego Int'l Airport, Lindbergh	1,887,346	99.6%	0.4%	0.0%	2,189,870	94.4%	5.0%	0.6%	-13.8%	5.2%	-4.7%	-0.6%
SEA	Seattle-Tacoma Intl. Airport	2,702,128	98.3%	1.6%	0.1%	2,985,815	96.8%	3.1%	0.1%	-9.5%	1.6%	-1.5%	0.0%
SFO	San Francisco Intl Airport	3,693,195	100.0%	0.0%	0.0%	4,063,135	100.0%	0.0%	0.0%	-9.1%	0.0%	0.0%	0.0%
SJU	Luis Munoz Marin Int'l Airport	1,026,888	99.9%	0.1%	0.0%	1,207,563	96.4%	3.5%	0.1%	-15.0%	3.6%	-3.4%	-0.1%
SLC	Salt Lake City Intl	1,489,212	99.8%	0.2%	0.0%	1,661,903	95.0%	4.3%	0.6%	-10.4%	4.8%	-4.2%	-0.6%
SMF	Sacramento International Airport	1,104,420	100.0%	0.0%	0.0%	1,343,033	99.9%	0.1%	0.0%	-17.8%	0.1%	-0.1%	0.0%
SNA	John Wayne Airport	890,627	100.0%	0.0%	0.0%	1,269,633	92.8%	6.1%	1.1%	-29.9%	7.2%	-6.1%	-1.1%
STL	Lambert St Louis International Airport	1,404,875	100.0%	0.0%	0.0%	1,598,951	98.0%	1.7%	0.2%	-12.1%	2.0%	-1.7%	-0.2%
TPA	Tampa International Airport	2,287,883	99.9%	0.1%	0.0%	2,994,824	91.3%	8.2%	0.4%	-23.6%	8.6%	-8.1%	-0.4%

III. Passenger Screening Wait Time Data

IV. Performance Highlights and Major Change Notes

Focus Airport	Focus Airport Name	Quarter 2 FY09				Relative Change (FY09 - FY08)			
		Total Throughput	% Passengers Waiting < 20 Minutes	% Passengers Waiting 20-30 Minutes	% Passengers Waiting > 30 Minutes	Total Throughput	% Passengers Waiting < 20 Minutes	% Passengers Waiting 20-30 Minutes	% Passengers Waiting > 30 Minutes
ATL	Hartsfield Atlanta International Airport	3,945,462	100.0%	0.0%	0.0%	-14.1%	18.3%	-14.4%	-3.9%
		-646,301 decreased					Improvement In Wait	Improvement In Wait	Improvement In Wait

Change: Significant outside resources (optimization teams, experienced managers/coaches) were deployed 4-9/08 to improve all aspects of screening operations.

ATL achieved 100.0% of its passengers waiting less than 20 minutes - an improvement of 18.3%. Throughput decreased by -14.1%

Reasons for [relative] significant change:

Passenger and business growth

- Reorganization of staffing - reduction of TSOs assigned to baggage and an increase in TSOs assigned to checkpoints
- Improved scheduling including shift bids on six month timetable, instead of annual. This increases flexibility to adjust schedules to operational and officer needs
- Improved infrastructure including: addition of 5 additional lanes, redesigned queues, integrated selectee lanes, and self select lanes

Focus Airport	Focus Airport Name	Quarter 2 FY09				Relative Change (FY09 - FY08)			
		Total Throughput	% Passengers Waiting < 20 Minutes	% Passengers Waiting 20-30 Minutes	% Passengers Waiting > 30 Minutes	Total Throughput	% Passengers Waiting < 20 Minutes	% Passengers Waiting 20-30 Minutes	% Passengers Waiting > 30 Minutes
MIA	Miami International Airport	3,619,225	99.9%	0.1%	0.0%	-4.8%	17.6%	-17.1%	-0.5%
		-182,209 decreased					Improvement In Wait	Improvement In Wait	Improvement In Wait

Change: MIA achieved 99.9% of its passengers waiting less than 20 minutes - an improvement of 17.6%. Throughput decreased by -4.8%

Reasons for [relative] significant change:

Processing capacity improved

- Total redesign of all checkpoints: Added 2-sided queue at Transport Document Checking (TDC), using 2 X-rays served by 1 Walk-Thru Metal Detector (a.k.a. 2:1 layout), optimizing divest and recompose roller lengths.
- Staffing changed to allocate Part Time and Split Shift TSO's during peak periods
- Local hiring (improved process allows TSA to quickly add and backfill new employees).

Focus Airport	Focus Airport Name	Quarter 2 FY09				Relative Change (FY09 - FY08)			
		Total Throughput	% Passengers Waiting < 20 Minutes	% Passengers Waiting 20-30 Minutes	% Passengers Waiting > 30 Minutes	Total Throughput	% Passengers Waiting < 20 Minutes	% Passengers Waiting 20-30 Minutes	% Passengers Waiting > 30 Minutes
DCA	Ronald Reagan Washington National AP	1,724,315	99.4%	0.2%	0.3%	-1.2%	-0.3%	0.0%	0.3%
		-21,444 decreased					Degradation In Wait	Degradation In Wait	Degradation In Wait

Change: DCA achieved 99.4% of its passengers waiting less than 20 minutes - a slight degradation in performance of -0.3%. Throughput decreased by -1.2%

The slight degradation in performance is due to the extraordinary influx of travelers to President Obama's historical inauguration. Approximately 5,200 passengers experienced a delay greater than 30 min. during 2Q FY09.

Reasons for [relative] significant change:

Processing capacity improved

- Total redesign of all checkpoints: Added 2-sided queue at Transport Document Checking (TDC), using 2 X-rays served by 1 Walk-Thru Metal Detector (a.k.a. 2:1 layout), optimizing divest and recompose roller lengths.
- Staffing changed to allocate Part Time and Split Shift TSO's during peak periods
- Local hiring (improved process allows TSA to quickly add and backfill new employees).

Notes: * The Change formula for throughput is = [(FY09-FY08)/FY08]; while the changes in percentage thresholds of 20 and 30 minutes are = [FY09% - FY08%].

TSA has modified the measure of wait from high-labor burden in sampling actual times to measured wait time indicators of 20 and 30 minutes.

This change allows the workforce to focus on security, since over 99% of passengers are being screened with wait times of less than 20 minutes (an improvement from 97% in FY07).

V. Conclusion

In conclusion, industry passenger travel in the second quarter of FY 2009 has declined 14.4 percent from the previous year, as measured by the checkpoint throughput (count of persons screened). Nationwide, TSA continues to be significantly below the average wait time standard of 10 minutes. Incidents of passenger wait times of 20 minutes or more were reduced to less than 0.5 percent in the Focus 40 airports.

VI. Appendix A: Glossary of Terms

2:1 Layout	Two X-ray served by one WTMD – reduces one Transportation Security Officer fixed position among other efficiency improvements at security checkpoints
9/11 Act	Implementing Recommendations of the 9/11 Commission Act (P. L. 110-53)
DHS	Department of Homeland Security
FLETC	Federal Law Enforcement Training Center
Focus 40	Set of forty (40) airports which represent the largest U.S. Airports under the Transportation Security Administration
FY	Fiscal Year
OMB	Office of Management and Budget
SAM	Staffing Allocation Model used by TSA to forecast passenger security screening demand, allocate and schedule TSOs
Throughput	Security screening demand which includes passengers and airline industry workers. In the context of checked baggage, it is the number of checked bags and packages screened by TSA
TIP	Threat Image Projection program that overlays threat images on to X-ray images continually testing TSO threat detection capabilities
TRX	TIP-Ready X-ray at a passenger security checkpoint
TSA	Transportation Security Administration
TSO	Transportation Security Officer
WBI	Whole-Body Imager detects possible threats on persons at security checkpoints
WTMD	Walk-through Metal Detection machine at the security checkpoint



Passenger Screening Wait Times

Fiscal Year 2009 Report to Congress

Fourth Quarter

December 24, 2009



Homeland
Security

Transportation Security Administration

Message from the Acting Administrator

December 24, 2009

I am pleased to present the Transportation Security Administration (TSA) Report to Congress on passenger screening wait times for the Fourth Quarter of Fiscal Year (FY) 2009. This report is required by the FY 2009 Department of Homeland Security Appropriations Act (P.L. 110-329), which directs TSA to submit airport wait time data on a quarterly basis for domestic airports with above average wait times and for the 40 busiest (Focus 40) airports.

Pursuant to congressional requirements, this report is being provided to the following Members of Congress:

The Honorable David E. Price
Chairman, House Appropriations Subcommittee on Homeland Security

The Honorable Harold Rogers
Ranking Member, House Appropriations Subcommittee on Homeland Security

The Honorable Robert C. Byrd
Chairman, Senate Appropriations Subcommittee on Homeland Security

The Honorable George V. Voinovich
Ranking Member, Senate Appropriations Subcommittee on Homeland Security

Inquiries relating to this report may be directed to me at (571) 227-2845 or to the Department's Acting Chief Financial Officer, Peggy Sherry, at (202) 447-5751.

Sincerely yours,

A handwritten signature in black ink, appearing to read "Gale D. Rossides".

Gale D. Rossides
Acting Administrator

Executive Summary

The Fiscal Year (FY) 2009 Department of Homeland Security Appropriations Act directs the Transportation Security Administration (TSA) to report to Congress passenger screening wait time data on a quarterly basis for domestic airports with above average wait times and for the 40 busiest (Focus 40) airports.

TSA compared passenger screening wait times for the Fourth Quarters of FY 2008 and FY 2009. The data show that at airports nationwide, 99.3 percent of passengers experienced wait times of less than 20 minutes, an increase of 0.1 percent from the 99.2 percent of passengers who experienced wait times of less than 20 minutes in the Fourth Quarter of FY 2008.

At the Focus 40 airports, the results were similar: 99.2 percent of passengers experienced wait times of less than 20 minutes, which was the same percentage of passengers who experienced wait times of less than 20 minutes in the Fourth Quarter of FY 2008.

TSA continues to maintain a 10-minute wait time standard.



Passenger Screening Wait Times Fiscal Year 2009, Fourth Quarter

Table of Contents

I. Legislative Requirement	1
II. Background	2
III. Passenger Screening Wait Time Data	3
IV. Conclusion	4
V. Appendix: Glossary of Terms	5

I. Legislative Requirement

The Fiscal Year (FY) 2009 Department of Homeland Security Appropriations Act (P.L. 110-329) states:

Consistent with prior years, TSA shall continue to submit airport wait time data on a quarterly basis for domestic airports with above average wait times and for the top 40 busiest airports. . As part of these reports, TSA shall explain any dramatic shift in wait times and what is being done to reduce wait times at these airports. TSA shall not alter its current 10 minute standard.

This report is submitted in accordance with that requirement.

II. Background

TSA collects throughput (the number of persons screened) data through counters located at the walk-through metal detector (WTMD) or Advanced Imaging Technology (AIT), formerly whole-body imager (WBI), at the entrance to each screening lane within a checkpoint.

Since 2004, TSA has reduced average wait times nationwide to less than 5 minutes through checkpoint process optimization and continuous improvement initiatives. Since September 11, 2008, TSA has focused on reducing passenger wait time incidents of 20 minutes or more. These incidents are reported along with the hourly throughput counts to each airport coordination center, which uploads the data to TSA's Performance Management Information System (PMIS) on a daily basis.

The wait time data contained in this report was generated from PMIS and compares wait time performance in the Fourth Quarter of FY 2009 to wait time data for the Fourth Quarter of FY 2008. The throughput information provides insight as to passenger travel demand and seasonal changes.

III. Passenger Screening Wait Time Data

Airport	Quarter 4 FY09				Quarter 4 FY08				Throughput Absolute Change (FY09-FY08) /FY08	Relative Change (FY09 - FY08)		
	Customer Throughput - Chpt, Date, Hr				Customer Throughput - Chpt, Date, Hr							
	Total Throughput	% Passengers Waiting < 20 Minutes	% Passengers Waiting 20-30 Minutes	% Passengers Waiting > 30 Minutes	Total Throughput	% Passengers Waiting < 20 Minutes	% Passengers Waiting 20-30 Minutes	% Passengers Waiting > 30 Minutes		% Passengers Waiting < 20 Minutes	% Passengers Waiting 20-30 Minutes	% Passengers Waiting > 30 Minutes
TSA	152,760,563	99.3%	0.6%	0.1%	161,204,771	99.2%	0.7%	0.1%	-5.2%	0.1%	-0.1%	0.0%
F40	111,780,165	99.2%	0.8%	0.1%	117,030,180	99.2%	0.8%	0.1%	-4.5%	0.0%	0.0%	0.0%
ATL	4,809,053	100.0%	0.0%	0.0%	4,971,682	99.0%	0.9%	0.1%	-3.3%	1.0%	-0.9%	-0.1%
BOS	4,068,968	100.0%	0.0%	0.0%	3,823,924	99.3%	0.5%	0.2%	6.4%	0.7%	-0.5%	-0.2%
BWI	2,435,973	99.7%	0.3%	0.0%	2,232,929	100.0%	0.0%	0.0%	9.1%	-0.2%	0.2%	0.0%
CLE	942,346	100.0%	0.0%	0.0%	1,096,573	98.9%	1.0%	0.0%	-14.1%	1.1%	-1.0%	0.0%
CLT	1,475,955	99.6%	0.3%	0.1%	1,546,381	99.7%	0.3%	0.0%	-4.6%	-0.2%	0.0%	0.1%
CVG	693,830	99.7%	0.2%	0.1%	628,597	99.9%	0.1%	0.0%	10.4%	-0.2%	0.1%	0.1%
DCA	1,968,508	99.9%	0.1%	0.0%	1,934,420	99.9%	0.1%	0.0%	1.8%	0.0%	0.0%	0.0%
DEN	3,562,601	96.3%	3.5%	0.2%	3,680,690	98.9%	1.0%	0.0%	-3.2%	-2.6%	2.5%	0.1%
DFW	4,960,429	100.0%	0.0%	0.0%	5,112,070	99.9%	0.1%	0.0%	-3.0%	0.1%	-0.1%	0.0%
DTW	2,284,369	100.0%	0.0%	0.0%	2,603,686	99.9%	0.1%	0.0%	-12.3%	0.1%	-0.1%	0.0%
EWR	4,270,303	98.1%	1.8%	0.2%	4,529,173	99.4%	0.5%	0.0%	-5.7%	-1.4%	1.2%	0.1%
FLL	2,332,469	100.0%	0.0%	0.0%	2,396,619	99.8%	0.2%	0.0%	-2.7%	0.2%	-0.2%	0.0%
HNL	1,888,570	100.0%	0.0%	0.0%	1,770,055	100.0%	0.0%	0.0%	6.7%	0.0%	0.0%	0.0%
IAD	2,300,381	100.0%	0.0%	0.0%	2,383,814	98.8%	1.2%	0.0%	-3.5%	1.2%	-1.2%	0.0%
IAH	2,895,321	100.0%	0.0%	0.0%	3,062,764	100.0%	0.0%	0.0%	-5.5%	0.0%	0.0%	0.0%
IND	997,684	100.0%	0.0%	0.0%	1,075,699	99.8%	0.2%	0.0%	-7.3%	0.2%	-0.2%	0.0%
JFK	6,368,343	99.9%	0.1%	0.0%	6,403,744	98.1%	1.6%	0.3%	-0.6%	1.8%	-1.6%	-0.3%
LAS	4,272,424	99.9%	0.1%	0.0%	4,544,720	100.0%	0.0%	0.0%	-6.0%	-0.1%	0.1%	0.0%
LAX	7,284,520	96.9%	2.9%	0.2%	8,345,997	98.1%	1.8%	0.1%	-12.7%	-1.2%	1.1%	0.1%
LGA	3,117,488	96.8%	2.7%	0.5%	3,150,179	97.9%	2.0%	0.2%	-1.0%	-1.1%	0.7%	0.3%
MCI	1,756,005	99.9%	0.0%	0.0%	1,762,540	99.9%	0.0%	0.1%	-0.4%	0.1%	0.0%	-0.1%
MCO	4,065,107	100.0%	0.0%	0.0%	4,114,976	100.0%	0.0%	0.0%	-1.2%	0.0%	0.0%	0.0%
MDW	1,688,341	96.2%	3.5%	0.4%	1,670,129	100.0%	0.0%	0.0%	1.1%	-3.8%	3.5%	0.4%
MIA	3,509,345	100.0%	0.0%	0.0%	3,668,147	99.3%	0.7%	0.0%	-4.3%	0.7%	-0.7%	0.0%
MSP	2,600,835	100.0%	0.0%	0.0%	2,504,164	99.9%	0.1%	0.0%	3.9%	0.1%	-0.1%	0.0%
OAK	1,409,208	100.0%	0.0%	0.0%	1,613,374	99.9%	0.1%	0.0%	-12.7%	0.1%	-0.1%	0.0%
ORD	5,456,053	99.2%	0.8%	0.0%	6,036,091	99.4%	0.6%	0.0%	-9.6%	-0.2%	0.2%	0.0%
PDX	1,702,538	100.0%	0.0%	0.0%	1,844,253	99.9%	0.1%	0.0%	-7.7%	0.1%	-0.1%	0.0%
PHL	3,035,801	100.0%	0.0%	0.0%	3,356,320	94.6%	5.2%	0.2%	-9.5%	5.4%	-5.2%	-0.2%
PHX	3,044,162	98.1%	1.7%	0.2%	3,372,057	99.8%	0.2%	0.0%	-9.7%	-1.6%	1.4%	0.2%
RDU	1,173,685	100.0%	0.0%	0.0%	1,253,754	99.8%	0.2%	0.0%	-6.4%	0.2%	-0.2%	0.0%
SAN	2,317,578	99.5%	0.5%	0.0%	2,421,830	96.9%	3.0%	0.1%	-4.3%	2.6%	-2.6%	-0.1%
SEA	3,686,542	95.9%	3.8%	0.3%	3,772,943	98.2%	1.7%	0.1%	-2.3%	-2.3%	2.1%	0.2%
SFO	4,899,215	99.5%	0.3%	0.2%	4,985,586	99.9%	0.1%	0.0%	-1.7%	-0.4%	0.3%	0.2%
SIU	1,066,006	100.0%	0.0%	0.0%	1,127,700	99.3%	0.7%	0.0%	-5.5%	0.7%	-0.7%	0.0%
SLC	1,336,439	99.9%	0.1%	0.0%	1,542,561	99.3%	0.7%	0.0%	-13.4%	0.6%	-0.6%	0.0%
SMF	1,273,887	100.0%	0.0%	0.0%	1,451,822	100.0%	0.0%	0.0%	-12.3%	0.0%	0.0%	0.0%
SNA	1,122,732	99.5%	0.5%	0.0%	1,174,587	100.0%	0.0%	0.0%	-4.4%	-0.5%	0.5%	0.0%
STL	1,629,840	100.0%	0.0%	0.0%	1,738,372	99.3%	0.7%	0.1%	-6.2%	0.7%	-0.7%	-0.1%
TPA	2,077,311	100.0%	0.0%	0.0%	2,325,258	99.7%	0.3%	0.0%	-10.7%	0.3%	-0.3%	0.0%

IV. Conclusion

In conclusion, industry passenger travel in the Fourth Quarter of FY 2009 has declined 5.2 percent from the previous year, as measured by the checkpoint throughput (count of persons screened). Nationwide, TSA continues to be significantly below the average wait time standard of 10 minutes. Incidents of passenger wait times of 20 minutes or more remained the same level (less than 1 percent) in the Focus 40 airports.

V. Appendix: Glossary of Terms

AIT	Advanced Imaging Technology (formerly WBI) detects threats on individuals at checkpoints
Focus 40	Set of 40 airports which represent the largest U.S. Airports under the Transportation Security Administration
FY	Fiscal Year
PMIS	Performance Management Information System
Throughput	Security screening demand which includes passengers, airline industry workers. In the context of checked baggage, it is the number of checked bags and packages screened by TSA
WBI	Whole-Body Imager
WTMD	Walk-through Metal Detection machine at the security checkpoint

FOR OFFICIAL USE ONLY



Screening Technology Maintenance and Utilities

Fiscal Year 2009 Report to Congress

July 1, 2009



Homeland
Security

Transportation Security Administration

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Message from the Acting Administrator

July 1, 2009

I am pleased to present the following report, "Screening Technology Maintenance and Utilities," which has been prepared by the Transportation Security Administration (TSA).

This document has been developed in response to a requirement in the Explanatory Statement which accompanies the Fiscal Year 2009 Department of Homeland Security Appropriations Act (P.L. 110-329). It provides an explanation of the costs involved with the screening technology employed by TSA. In addition, the report describes initiatives being taken by TSA to counteract the costs associated with the screening technologies.

This report is being provided to:

The Honorable David E. Price
Chairman, House Appropriations Subcommittee on Homeland Security

The Honorable Harold Rogers
Ranking Member, House Appropriations Subcommittee on Homeland Security

The Honorable Robert C. Byrd
Chairman, Senate Appropriations Subcommittee on Homeland Security

The Honorable George V. Voinovich
Ranking Member, Senate Appropriations Subcommittee on Homeland Security

Please do not hesitate to contact me at (571) 227-2845 or the Department's Acting Chief Financial Officer, Peggy Sherry, at (202) 447-5751 if we may be of further assistance.

Sincerely yours,



Gale D. Rossides
Acting Administrator
Transportation Security Administration

Executive Summary

This report responds to a requirement that accompanies the Fiscal Year (FY) 2009 Department of Homeland Security Appropriations Act (P.L. 110-329) to report on maintenance and utilities costs for screening equipment and identifies ways to curb future cost growth.

This report provides an overview and status of the Transportation Security Administration's (TSA's) screening equipment maintenance program and explains the cost escalation related to this equipment. It also identifies strategies TSA is pursuing to control unit maintenance costs in the future while preserving the availability of screening equipment technologies, including:

- Expansion of competition in the security screening industry.
- Development of a Remote Maintenance Monitoring (RMM) capability.
- Life cycle replacement of aging and unreliable machines.
- Improved reliability and maintainability specifications for new screening equipment.
- A review of excess capacity.



Screening Technology Maintenance and Utilities

Table of Contents

I. Legislative Requirement	1
II. Overview and Status of Screening Equipment Maintenance Program	2
III. Explanation of Cost Escalation	3
IV. Cost Control Initiatives	5
V. Conclusion	7

FOR OFFICIAL USE ONLY

I. Legislative Requirement

This report is provided in compliance with the Explanatory Statement which accompanies the Fiscal Year (FY) 2009 Department of Homeland Security (DHS) Appropriations Act (P.L. 110-329), excerpted as follows:

The bill provides \$305,625,000 for Screening Technology Maintenance and Utilities, of which \$4,400,000 can be used for costs related to the disposal of screening equipment no longer in service. Because of persistent cost escalations in this area, TSA shall provide a report to the Committees on maintenance and utility costs for screening technologies and identify ways that these costs may be controlled in the future.

II. Overview and Status of Screening Equipment Maintenance Program

TSA's mission is to safeguard the Nation's transportation systems. Maintenance is essential to preserve the operational capability of security technology equipment. Equipment failures can increase when maintenance is neglected or delayed. When equipment fails, Transportation Security Officers (TSOs) are deprived of using their advanced technological capabilities for screening baggage and passengers to detect unauthorized weapons, explosives, incendiaries and other destructive devices, items or substances. The availability of security screening equipment preserves airport efficiency and minimizes impact on the traveling public.

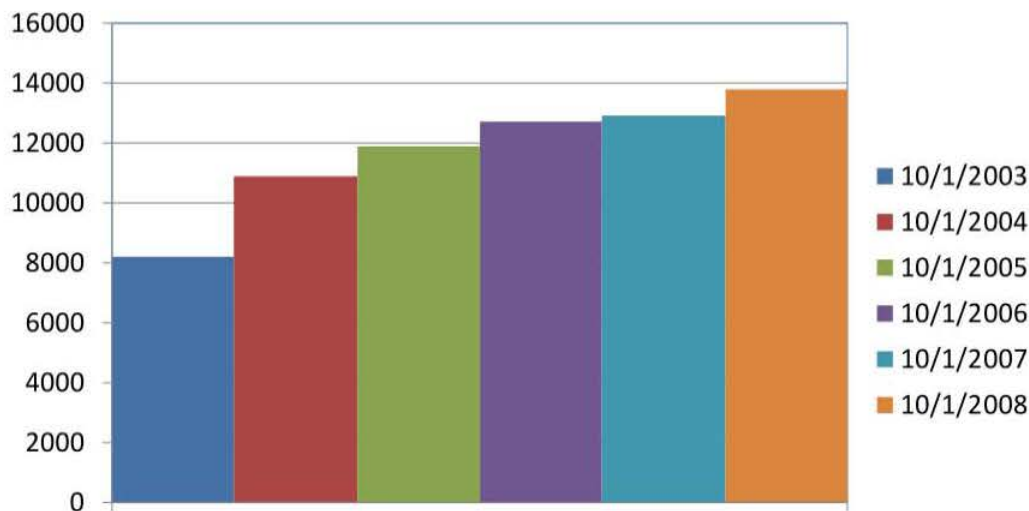
TSA obtains maintenance services for over 13,500 items of security screening equipment at our Nation's airports through contracts with Original Equipment Manufacturers (OEM) and a third-party maintenance provider. These contracts were awarded between October 2004 and March 2005 with a five-year period of performance, so each will expire in the next 9-15 months. These contracts have fixed prices for different types and models of equipment that provide one year of preventive and corrective maintenance (parts and labor).

Contract (service-level agreement) performance requirements are specified as equipment Mean Down Time (MDT) stated in hours. MDT is calculated and reported monthly across the population (fleet) of each specific type of technology equipment (*e.g.*, CTX-2500 Explosives Detection Systems (EDS)). Contract penalties are assessed if equipment down time exceeds the MDT requirement. The contractors are generally successful in meeting these requirements.

III. Explanation of Cost Escalation

Because the TSA maintenance strategy employs fixed-price contracts for different types of equipment, annual maintenance costs are largely dependent on the quantity of equipment installed at airports. In FY 2008, maintenance costs were approximately \$260 million. The costs of these fixed-price maintenance contracts grew to approximately \$305 million in FY 2009. The bulk of this growth was attributable to increased quantities of equipment at the airports, with a modest increase attributable to the anticipated cost of a new, more demanding Service Level Agreement performance metric.

Fielded Transportation Security Equipment by Fiscal Year



An increase in fielded security equipment has a direct correlation to the maintenance costs. The number of fielded Explosives Detection Systems (EDS) units grew by 16 percent from FY 2008 to FY 2009. TSA expects further increases from FY 2009 to FY 2010 as TSA fields new technologies and continues to improve existing security coverage. These additional security equipment expansions will increase the bottom line maintenance costs in future fiscal years.

FOR OFFICIAL USE ONLY

These equipment procurement increases directly affect the maintenance budget for the life of the machines.

The other factor that contributed to the cost growth between FY 2008 and FY 2009 is the change in the service-level agreement performance metric from MDT at the fleet level to Operational Availability at the airport level. While the contractors have been largely successful in meeting contract MDT requirements, measuring MDT across the fleet population tends to reward good performance at large airports with large equipment installations, while smaller or more remote airports are given less priority. In order to address this inequity and provide better equipment availability at *every* airport, a contract modification is pending to change the performance metric from *fleet-wide* MDT to *airport-level* Operational Availability. The proposed modification includes:

- Contract penalties will be imposed if *any* airport fails to make its goal. This change is expected to be implemented in the late second quarter or early third quarter FY 2009 timeframe for Explosives Detection Systems built and maintained by L3 Communications and General Electric.
- Because this more demanding readiness requirement will require changes in the number and distribution of contractor maintenance and logistics support resources, a small price increase was anticipated and included in the FY 2009 budget request.

Acceleration of program funding, changes to the baseline program or requirements to field new technologies that supplement existing capabilities will all cause growth in the TSA maintenance budget. Once the fleet of fielded equipment is stable, the recent growth trend will cease, and increases from the base will be for inflation and other fact-of-life requirements.

IV. Cost Control Initiatives

Given the contract pricing structure of firm fixed prices per equipment, annual maintenance costs are most directly affected by the quantity of security equipment installed at airports. Increases in the FY 2008 and FY 2009 Electronic Baggage Screening Program (EBSP)/Passenger Screening Program (PSP) procurement and installation budgets drive an increase in maintenance requirements in subsequent years, over and above the planned budget baseline.

TSA plans to continue with firm fixed-price maintenance contracts to safeguard the government against potential cost increases associated with maintenance of aging technology systems. Despite near-term growth in the overall requirement for maintenance funding due to increased equipment quantities, TSA is seeking to control and reduce maintenance costs within the constraints of the firm fixed-price contracts.

Some of the current initiatives include expansion of competition in the security screening industry, development of a Remote Maintenance Monitoring (RMM) capability, life-cycle replacement of aging and unreliable machines, improved reliability and maintainability specifications for new screening equipment and a review of excess capacity.

Competition: As procurement competition increases, TSA will consider maintenance costs as a source selection criterion for new EBSP and PSP procurements. When there is competition for a new procurement, TSA will establish a criterion that will rate potential vendors on their projected maintenance costs over the life cycle of the equipment. This will enable TSA to procure equipment from the vendors that meet the performance specifications and have the best life-cycle cost value to TSA. Also, the next third-party maintenance contract for checkpoint screening equipment will be competitively awarded in September 2009.

Remote Maintenance Monitoring: As a long-term initiative, TSA has a program to increase the RMM capabilities of current and future security equipment. As part of this initiative, TSA is developing the ability within the equipment to establish and monitor performance parameter thresholds. RMM will enable TSA to monitor the established performance parameters and initiate predictive corrective maintenance actions on a more scheduled and less disruptive basis as the equipment's performance approaches the performance thresholds. It will also provide the ability to push electronically some corrective maintenance actions such as restarts and software updates. These RMM capabilities should significantly improve the operational availability of the security equipment to TSA, reduce the number of unscheduled visits to the facilities and consequently reduce maintenance costs to the maintenance service provider. TSA will then use accumulated maintenance service provider cost data for the negotiation of reduced maintenance unit costs for future maintenance contracts. As mentioned, this is a long-term initiative and the first benefits to TSA are improved operational availability and less disruption to the facility.

FOR OFFICIAL USE ONLY

operations. TSA does not expect to realize any cost savings from this initiative until 2011 or later.

Life-cycle replacement: A life-cycle replacement program for EDS has been initiated in FY 2009 that will address older machines that may be approaching the end of their useful life, or that may be growing unreliable. By replacing these machines in a methodical fashion and achieving demonstrated improvements in machine reliability, TSA hopes to leverage future price negotiations with maintenance providers, since the age of the fleet being maintained will be reduced and the quality increased. Also, to the degree that airport configurations allow, maintenance costs and the reliability of replacement machines will be a factor in the selection of replacement equipment. For example, if an existing machine can be replaced by a more affordable, more reliable machine from a different manufacturer (*e.g.*, CT80 vs. CTX2500/5500), cost avoidance impacts are immediate.

Reliability and Maintainability Specification: The TSA Life-Cycle Support Manager and Maintenance Manager are interacting with engineering and procurement personnel to a greater degree to ensure that supportability considerations are incorporated early into equipment specifications. More stringent reliability and maintainability requirements up front will reduce maintenance requirements, leading to better contract price negotiation positions, reduced costs and better equipment availability for the benefit of TSOs in the field. This is a long-term initiative, with benefits likely to be achieved in 2012 and beyond.

Excess Capacity: TSA is reviewing security screening equipment utilization at selected airports that may have been designed with excess capacity during the initial roll-out in 2002. If these reviews reveal capacity in excess of that required for redundancy and surge capacity, TSA will identify equipment candidates for decommissioning, removal, redeployment or disposal. This will have an immediate impact on the cost of maintenance.

Pricing: Current maintenance contracts have fixed unit prices that apply regardless of the quantity of equipment supported. As equipment quantities grow, the marginal cost of providing maintenance may decrease. In future contracts, TSA will explore the option of establishing a tiered pricing structure based on variable quantities of equipment. Follow-on EBSP maintenance contracts are scheduled for award in the second quarter of FY 2010.

V. Conclusion

TSA's maintenance strategy of providing preventive and corrective maintenance via fixed-price contracts represents a cost-effective means of ensuring maximum availability of security screening equipment technologies. Because the cost of maintenance is directly related to the numbers of machines fielded, the recent increase in quantities of fielded equipment has predictably caused a corresponding increase in the overall size of the TSA security screening equipment maintenance budget. As long as the numbers of fielded equipment continues to grow, the overall level of the maintenance budget will also grow. When the size of the fleet becomes stable, the rate of growth will flatten to include inflation and other fact-of-life increases, and the effects of the cost avoidance initiatives discussed in this document will become apparent.



Annual Report on Transportation Security

January 12, 2010



Homeland
Security

*Transportation Security
Administration*

Foreword

I am pleased to transmit the Annual Report on Transportation Security. This report combines two reports previously submitted separately: the *Annual Report to Congress on Transportation Security* and the *Periodic Progress Report on the National Strategy for Transportation Security*. The report encompasses all modes of transportation to reflect the specific responsibilities assigned by the Department of Homeland Security (DHS), through the Homeland Security Presidential Directive-7 and the National Infrastructure Protection Plan process. The report also incorporates, as an appendix, a progress report evaluating actions taken in eight specific areas to enhance the security of transportation as required in Section 109 of the Aviation and Transportation Security Act.

To meet the ever-changing threat environment, the Transportation Security Administration (TSA) makes significant efforts to become an even more flexible risk management-based organization. TSA continues an intensive effort to better utilize our field forces and resources across all modes of transportation. We are providing better and smarter security and increasing the efficiency of our resources. We added additional levels of security, with employees performing more advanced security functions. TSA is focused beyond the physical checkpoint, expanding our sphere of impact to look more carefully at people to identify those with hostile intent, create multiple opportunities to detect terrorists, and leverage the capabilities of our workplace, our partners, and our technology.

Pursuant to congressional requirements, this report is being provided to the following members of Congress:

The Honorable Joseph Biden
President of the Senate

The Honorable Nancy Pelosi
Speaker of the House

The Honorable Harry Reid
Senate Majority Leader

The Honorable Mitch McConnell
Senate Minority Leader

The Honorable John Boehner
House Minority Leader

The Honorable Daniel K. Inouye
Chairman, Commerce, Science, and Transportation Committee

The Honorable Kay Bailey Hutchison
Ranking Member, Commerce, Science, and Transportation Committee

The Honorable Joseph I. Lieberman
Chairman, Homeland Security and Governmental Affairs Committee

The Honorable Susan M. Collins
Ranking Member, Homeland Security and Governmental Affairs Committee

The Honorable Bennie G. Thompson
Chairman, Homeland Security Committee

The Honorable Peter T. King
Ranking Member, Homeland Security Committee

The Honorable James L. Oberstar
Chairman, Transportation and Infrastructure Committee

The Honorable John L. Mica
Ranking Member, Transportation and Infrastructure Committee

If I may be of further assistance, please do not hesitate to contact me or the TSA Office of Legislative Affairs at (571) 227-2717.

Sincerely yours,

A handwritten signature in cursive script, reading "Gale D. Rossides".

Gale D. Rossides
Acting Administrator

Executive Summary

The threat environment in transportation remains high and the Transportation Security Administration's (TSA) challenge has never been greater. To meet the ever-changing threat environment, TSA is taking significant steps to become an even more flexible, risk-managing organization by better utilizing security resources across all modes of transportation. With our Federal, State, local, tribal, and private sector security partners, we are providing better, smarter, and more efficient security for more travelers, adding more levels of security, and performing more advanced security functions. Finally, we are extending security beyond the physical checkpoint and more comprehensively across transportation modes to identify and deter those with hostile intent.

2008 Highlights include:

- Deployed Visible Intermodal Prevention and Response (VIPR) Teams to enhance screening, look for suspicious behavior, and act as visible deterrents in multiple transportation sectors. Approximately 60 percent of VIPR teams are dedicated to the aviation sector, including air cargo, commercial aviation, and general aviation; and 40 percent of operations to surface modes, including highways, freight rail, pipelines, mass transit, and maritime.
- Reduced Transportation Security Officer (TSO) full-time and part-time voluntary attrition for the fourth straight year. Full-time attrition decreased from 13.6 percent in 2004 to 10.8 percent in 2008; part-time attrition from 57.8 percent in 2004 to 31.8 percent in 2008.
- Trained 1,522 Behavior Detection Officers at 119 airports; certified Bomb Appraisal Officers for placement at 103 airports; trained and certified 424 Security Training Instructors; and trained over 13,088 new TSOs to enhance airport security nationwide.
- Vetted over 7 million people per day; adjudicated over 12,000 cases per week; and responded to over 750 redress requests a week in the transportation systems sector.
- Certified and began deploying reduced-size Explosives Detection Systems that screen over 200 bags per hour.
- Implemented the Certified Cargo Shipper Program that achieved 50 percent screening of domestic outbound and international inbound air cargo transported on passenger aircraft by February 2009, and is positioned to achieve 100 percent screening of domestic outbound by August 2010.
- Finalized regulations for Secure Flight, rail security, and air cargo.
- Participated in award of approximately \$804 million to State and local governments for programs and equipment that help to manage risk. The Transit Security Grants Program, which funded \$389 million in 2008, is the centerpiece of TSA's strategy to close security gaps.

This report is intended to be a high-level transportation security overview that introduces new concepts, ongoing efforts, and provides the progress and status of key programs, projects, and activities for 2008. It combines two transportation security reports with similar requirements into a single report and includes, as an appendix, a progress report on enhanced security

measures, as required by Section 109 of the Aviation and Transportation Security Act (ATSA), P.L. 107-71 (2001). The document describes the progress made in transportation security in calendar year 2008 previously submitted as the *Annual Report on Transportation Security*, required by 49, U.S.C. § 44938, and in fiscal year 2008 previously submitted as the *Periodic Progress Report on the National Strategy for Transportation Security (NSTS)*, required by title 49 U.S.C. § 114(t), amended by Section 1202(c) of the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act), P.L. 110-53. Consistent with the previous years' submissions, some requirements of the law are not included (*i.e.*, 49 USC § 44938(a)(6)-(9)).

The requirement to discuss the status of recommendations of the President's Commission on Aviation Security and Terrorism (created by Executive Order 12686) is omitted as the recommendations of this 1990 report have been fully integrated into transportation security planning and reinforced by subsequent laws such as ATSA and the Homeland Security Act of 2002. The requirement to discuss an "Assessment of Financial and Staffing Requirements" is not specifically addressed because it is included in budgetary and other required submissions from the Department of Homeland Security. Maritime transportation security activities are addressed in detail in a separate report required by section 110(a) of the Maritime Transportation Security Act of 2002, P.L. 107-295.

Table of Contents

1.	Legislative Requirement	1
2.	Background	3
3.	Assessment of Trends and Developments in Terrorist Activities, Methods, and Other Threats to Transportation	4
4.	Transportation Security Update	5
4.1	Aviation	5
4.1.1	Commercial Airlines	5
4.1.2	Commercial Airports	6
4.1.3	General Aviation	6
4.1.4	Air Cargo	7
4.2	Mass Transit and Passenger Rail	8
4.3	Freight Rail	9
4.4	Highway and Motor Carrier	11
4.5	Maritime	12
4.6	Pipeline	13
4.7	Intermodal Transportation Interconnectivity	15
5.	Research, Engineering, and Development Activities Related to Transportation Security	16
5.1	Screening and Inspection - Passengers	16
5.2	Screening and Inspection – Checked Baggage	17
5.3	Screening and Inspection – Cargo	17
5.4	Infrastructure and Conveyance Protection	17
5.4.1	Infrastructure Protection	17
5.4.2	Conveyance Protection	18
5.4.3	Improved Materials and Methods of New/Existing Structures	18
6.	Cooperative Efforts with Domestic and Foreign Security Partners	18
6.1	Other U.S. Departments, Agencies, Instrumentalities and State and Local Authorities	18
6.2	Foreign Transportation and Security Authorities	19
7.	Budget, Staffing and Grants	21
7.1	An Accounting of DHS Personnel Working on Transportation Security	21
7.2	Accounting of Funding in the President’s Budget for Transportation Security	24
7.3	Reducing Risks through Security Grants	24
8.	Conclusion/DHS Action Plan	27
Appendices		
	Appendix (A) - 2008 Report on Enhanced Security Measures	A-1
	Appendix (B) - List of Acronyms	B-1

1. Legislative Requirement

This report responds to the requirements set forth in the following legislative requirements:

Annual Report on Transportation Security: 49, U.S.C. § 44938.

(a) Transportation Security. Not later than March 31 of each year, the Secretary of [Homeland Security]¹ shall submit to Congress a report on transportation security with recommendations the Secretary considers appropriate. The report shall be prepared in conjunction with the biennial report the [Administrator, Transportation Security Administration] submits under subsection (b) of this section in each year the [Administrator] submits the biennial report, but may not duplicate the information submitted under subsection (b) or section 44907(a)(3) of this title. The Secretary may submit the report in classified and unclassified parts. The report shall include:

- (1) an assessment of trends and developments in terrorist activities, methods, and other threats to transportation;
- (2) an evaluation of deployment of explosive detection devices;
- (3) recommendations for research, engineering, and development activities related to transportation security, except research engineering and development activities related to aviation security to the extent those activities are covered by the national aviation research plan required under section 44501(c) of this title;
- (4) identification and evaluation of cooperative efforts with other departments, agencies, and instrumentalities of the United States Government;
- (5) an evaluation of cooperation with foreign transportation and security authorities;
- (6) the status of the extent to which the recommendations of the President's Commission on Aviation Security and Terrorism have been carried out and the reasons for any delay in carrying out those recommendations;
- (7) a summary of the activities of the Director of Intelligence and Security in the 12-month period ending on the date of the report;
- (8) financial and staffing requirements of the Director;
- (9) an assessment of financial and staffing requirements, and attainment of existing staffing goals, for carrying out duties and powers of the [Administrator] related to security; and
- (10) appropriate legislative and regulatory recommendations.

(b) Screening and Foreign Air Carrier and Airport Security. The [Administrator] shall submit biennially to Congress a report:

- (1) on the effectiveness of procedures under section 44901 of this title;
- (2) that includes a summary of the assessments conducted under section 44907(a) (1) and (2) of this title; and

¹ Functions and responsibilities of the Secretary of Transportation and the Undersecretary of Transportation for Security were transferred to the Secretary of Homeland Security and the Administrator of the Transportation Security Administration by operation of law pursuant to the Homeland Security Act of 2002, P.L. 107-296.

(3) that includes an assessment of the steps being taken, and the progress being made, in ensuring compliance with section 44906 of this title for each foreign air carrier security program at airports outside the United States:

- (A) at which the Under Secretary decides that Foreign Security Liaison Officers are necessary for air transportation security; and
- (B) for which extraordinary security measures are in place.

Periodic Progress Report: 49 U.S.C. § 114(t)(4)(C), as amended by Section 1202(c) of the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act)

(i) Requirement for Report – Each year, in conjunction with the submission of the budget to Congress under section 1105(a) of title 31, United States Code, the Secretary of Homeland Security shall submit to the appropriate congressional committees an assessment of the progress made on implementing the National Strategy for Transportation Security, including the transportation modal security plans.

(ii) Content – Each progress report submitted under this subparagraph shall include, at a minimum, the following:

(I) recommendations for improving and implementing the National Strategy for Transportation Security and the transportation modal and intermodal security plans that the Secretary of Homeland Security, in consultation with the Secretary of Transportation, considers appropriate.

(II) an accounting of all grants for transportation security, including grants and contracts for research and development, awarded by the Secretary of Homeland Security in the most recent fiscal year and a description of how such grants accomplished the goals of the National Strategy for Transportation Security.

(III) an accounting of all:

(aa) funds requested in the President’s budget submitted pursuant to section 1105 of title 31 for the most recent fiscal year for transportation security, by mode;

(bb) personnel working on transportation security by mode, including the number of contractors; and

(cc) information on the turnover in the previous year among senior staff of the Department of Homeland Security, including component agencies, working on transportation security issues. Such information shall include the number of employees who have permanently left the office, agency, or area in which they worked, and the amount of time that they worked for the Department.

(iii) Written explanation of transportation security activities not delineated in the national strategy for transportation security. At the end of each fiscal year, the Secretary of Homeland Security shall submit to the appropriate congressional

committees a written explanation of any Federal transportation security activity that is inconsistent with the National Strategy for Transportation Security, including the amount of funds to be expended for the activity and the number of personnel involved.

Enhanced Security Measures: Section 109(b) of the Aviation and Transportation Security Act

Report. Not later than 6 months after the date of enactment of this Act, and annually thereafter until the [Administrator] has implemented or decided not to take each of the actions specified in subsection (a), the [Administrator] shall transmit to Congress a report on the progress of the [Administrator] in evaluating and taking such actions, including any legislative recommendations that the Under Secretary may have for enhancing transportation security.

2. Background

TSA is mandated to protect all modes of the transportation system and ensure the freedom of movement for people and commerce. This mission is accomplished largely by a consortium of Federal, State, local, and private entities optimizing resources in a risk-based approach to security. In addition to coordination, TSA provides inspectors, surveillance, and other methods of screening and threat detection programs. These combined efforts play an essential role in the U.S. Department of Homeland Security's (DHS) mission to prevent terrorist acts within the United States, to reduce vulnerability to terrorism, and to minimize the damage from potential attacks. Key risk reduction activities include:

- **Security Vetting.** Conducting security threat assessments of workers, frontline employees, travelers, and shippers.
- **Securing Critical Infrastructure.** Preventing terrorist attacks by protecting critical elements of the transportation system and strengthening aviation, surface, and maritime assets to withstand incidents and recovery from an all-hazard event.
- **Risk Mitigating Operating Practices.** Reducing specific risk within a system by standardizing security activities that implement security programs.
- **Unpredictable Operational Deterrence.** Designing security activities to introduce elements of random and unpredictable operational deterrence to decrease the ability of actors with malicious intent to evaluate and predict security practices.
- **Screening of Workers, Travelers, and Cargo.** Screening, either physically or virtually, individuals, baggage, and cargo that pass through or operate in the transportation system.
- **Security Awareness and Response Training.** Training transportation workers to be security-conscious and aware of the security environment. Preparing workers to meet all-hazard events is a critical element of security and sector resiliency.
- **Preparedness and Response Exercises.** Conducting multimodal drills and exercises to mitigate risk in the Transportation Systems Sector (the Sector). Augmenting the ability of frontline employees and first responders to act quickly during and after an incident.
- **Public Awareness and Preparedness.** Increasing public and stakeholder awareness of the sector's security efforts through stakeholder information sharing, public announcements

within the transportation system, and other means of communicating to the public how to prevent and respond to security incidents.

- **Leveraging Technology.** Using technological advances to improve security effort, increase the efficiency of screening passengers and cargo, and decrease the intrusiveness of security practices without reducing their efficacy.
- **Transportation Industry Security Planning.** Raising the security baseline and increasing the amount and quality of security plan development, including business continuity planning in the transportation industries.
- **Security Programs and Vulnerability Assessments.** Evaluating the vulnerability of critical transportation infrastructure is a key element to inform strategic and investment decisions to reduce risk across the Sector.

TSA, its government partners, industry owners, and operators have increased vigilance by continuing to exchange real-time information and by focusing on threat detection and preparedness measures to improve security and resilience of the transportation system.

3. Assessment of Trends and Developments in Terrorist Activities, Methods, and Other Threats to Transportation

Although no international terrorist attacks have occurred in the United States since September 11, 2001, intelligence continues to indicate that al-Qa'ida and other affiliated terrorist organizations have an undiminished intent to conduct attacks inside the United States. Successful attacks against U.S. transportation systems would satisfy al-Qa'ida's main goals for attacks on the homeland: mass casualties, visually dramatic destruction, significant damage to the U.S. economy, and fear among the U.S. public. TSA continues to receive a large number of reports on suspicious incidents and possible surveillance of the U.S. transportation system. Such activity may indicate efforts by terrorists to identify weaknesses in the U.S. transportation infrastructure and to plan an attack strategy.

Despite successes in the global war on terrorism, al-Qa'ida continues to plot and prepare for major attacks inside the United States. According to the July 2007 National Intelligence Estimate, *The Terrorist Threat to the U.S. Homeland*, which assessed the terrorist threat from 2007-2010, al-Qa'ida's plots targeting the U.S. homeland are likely to focus on prominent political, economic, and infrastructure targets. Transportation is considered the most threatened U.S. infrastructure, and is likely to figure prominently in al-Qa'ida's future plans. Despite the post-9/11 security enhancements, al-Qa'ida continues to view U.S. civil aviation as a top operational objective and as a prized strategic target.

Overseas, al-Qa'ida and other terrorist groups have continued to launch attacks against U.S. and allied interests. Some of these attacks have targeted transportation systems, including the bombings of mass transit and rail systems in Madrid, Spain (2004) and London (2005), the disrupted plot to blow up passenger aircraft over the Atlantic Ocean (2006), the bombing of the passenger terminal at Scotland's Glasgow International Airport (2007), and the attack on the Chatrapati Shivaji Terminus railway station among other sites in Mumbai, India (2008).

According to the February 2008 *Annual Threat Assessment of the Director of National Intelligence for the Senate Select Committee on Intelligence*, al-Qa'ida has been able to retain a safe haven in the Federally Administered Tribal Areas of Pakistan. It continues to forge and

maintain ties with jihadists around the globe, including in Europe, the Levant, North and East Africa, the Arabian Peninsula, and in South and East Asia. Al-Qa'ida uses the Federally Administered Tribal Areas as a location to train new terrorist operatives, including the influx of Western recruits into the region since mid-2006. This could allow al-Qa'ida to improve its capability to conduct attacks on transportation interests in the United States and overseas.

Autonomous extremist cells that draw inspiration from al-Qa'ida, but operate independently, remain a serious threat. Small, "homegrown" extremist cells carried out the Madrid bombings (2004), the London bombings (2005), and the attack on Glasgow International Airport (2007). The disrupted plot to blow up fuel pipelines and storage tanks at John F. Kennedy International Airport in New York (2007) served as a reminder that the United States is not immune from such grassroots extremism. TSA remains alert, as well, to the potential threat posed by U.S. domestic extremists, including special interest terrorist groups, extremist groups, anarchist groups, and individuals acting alone.

The most likely method for terrorist attacks against the transportation system remains improvised explosive devices (IEDs), which are used in the majority of attacks overseas and are likely to remain the most common method in the near future. Conventional small arms and easy-to-acquire explosive precursors, such as hydrogen peroxide, are also a concern and have been used in recent attacks on the transportation system.

4. Transportation Security Update

The Transportation Systems Sector is segmented into six key subsectors, or modes, which operate independently within both regulated and non-regulated environments, yet are also highly interdependent. Such interdependence is a defining characteristic of the transportation system. The six modes — aviation, mass transit and passenger rail, freight rail, highway and motor carrier, maritime, and pipeline — all contribute to transporting people, food, water, medicines, fuel, and other commodities.

The asset categories and their corresponding security priorities form the basis of each modal security plan. The following sections provide a summary of progress on the key priorities established in the 2008 modal plans.

4.1 Aviation

Aviation is a vital component of the national economy, encompassing both private and public entities dedicated to achieving a comprehensive and integrated national approach towards aviation security. The Sector places primary emphasis on security risks associated with:

- ☐ Using aircraft as weapons, as in the 9/11 attacks,
- ☐ Aircraft becoming targets, as in the case of Pan American World Airways flight 103,
- ☐ Airport facilities, and
- ☐ The National Airspace System.

4.1.1 Commercial Airlines

- ☐ Air Carrier Risk Analysis. Risk analyses were completed on 78 U.S. air carriers resulting in the development of a strategy to improve compliance with TSA security

programs and lower the risk to air carriers conducting operations outside of the United States in areas requiring extraordinary security measures.

- ❑ Comprehensive Air Carrier Inspection Protocol. A protocol was developed that provides a comprehensive top-to-bottom inspection and review of all aspects of an air carrier's compliance with its security program(s).
- ❑ Special Emphasis Inspection for No-Fly List Compliance. Air carrier systems were inspected to ensure compliance with a Security Directive preventing persons on the No-Fly list from boarding aircraft.
- ❑ Airspace Security. Airline flight crews entering, leaving, or over-flying U.S. airspace were vetted against terrorist-related information using computerized vetting and matching analysis to assess potential threats of terrorists posing as cleared aviation personnel.

4.1.2 Commercial Airports

- ❑ Airport Employee Screening. Pilot projects were coordinated to demonstrate various methods to achieve 100 percent screening of airport employees. The projects were conducted between May 5, 2008, and July 2008, at seven airports of various sizes and geographic locations. A draft final report of findings is currently in review.
- ❑ Biometric Access Controls. Multi-agency efforts were coordinated to expand use of biometric access controls at commercial airports.
- ❑ Aviation Credential Interoperable Solution. TSA and DHS are partnering to develop the Aviation Credential Interoperable Solution, which will enhance certain aspects of credentialing and access control methodologies, and improve processes and devices to strengthen access control from registration/enrollment and vetting through physical access.
- ❑ Man-Portable Air Defense Systems (MANPADS) Vulnerability Assessments (MVA). This program conducts routine and special assessments and awareness training at large and higher-risk domestic and international airports. Self-assessment guides assist other airports in conducting MVAs. All domestic airports have completed MVA and MANPADS Mitigation Plans.

4.1.3 General Aviation

- ❑ International General Aviation (GA) Security. TSA is working in coordination with its international security partners (foreign countries) to establish a strong GA security foundation within the global community and harmonize efforts where practical. These efforts have consisted of information sharing on various projects and initiatives, as well as frequent participation in international GA security seminars (Ukraine - September 2008, Australia - November 2008, and Mexico - December 2008).
- ❑ GA Airport Vulnerability Assessment. The 9/11 Act directed TSA to develop a standardized threat and vulnerability assessment program for GA airports that will help identify vulnerabilities at GA airports and serve as a foundation on which to

build a GA grant program. GA Airport Vulnerability Survey development was completed and will be implemented in 2009.

- ❑ Large Aircraft Security Program (LASP) Notice of Proposed Rulemaking (NPRM). TSA issued the LASP NPRM in October 2008, designed to mitigate the threat of terrorist exploitation of large aircraft as a weapon against key assets and critical infrastructure. Once final, the LASP will require certain airport operators and U.S. operators of aircraft over a specified maximum takeoff weight to adopt a security program.
- ❑ Positive Pilot Identification (PPID). The PPID program is designed to address concerns with the frequent inability of ground stations to identify airmen operating GA aircraft in or near the National Airspace System. The Aircraft Communications Addressing and Reporting System (ACARS) was developed in coordination with security partners (government and industry stakeholders) to provide data communications between aircraft and ground stations. ACARS was initially used by commercial airlines but is now used by many general aviation operators through a subscription service from Aeronautical Radio, Incorporated (ARINC).
- ❑ Secure Fixed Base Operator (SFBO). The SFBO program is a TSA proof-of-concept initiative designed to strengthen the security of GA operations through private sector implementation of security measures at foreign FBO locations for flights operating to the United States. This program is a voluntary public-private partnership that provides a mechanism for verifying the identities of persons traveling onboard GA aircraft and strengthening the security of the operating area. In 2008, SFBO pilots were implemented in Shannon, Ireland; Anchorage, Alaska; Le Bourget, France; Luton, UK; Hong Kong, China; and Tokyo, Japan. The SFBO project is linked to PPID, assigning participating airmen identification badges to scan at the SFBO. It also vets passengers and crew prior to boarding at international locations.

4.1.4 Air Cargo

As mandated by the 9/11 Act, TSA is developing and implementing a system to screen 100 percent of air cargo loaded onto passenger aircraft, which provides a level of security commensurate with that of passenger checked baggage. TSA and its security partners are pursuing a number of initiatives to aid industry in achieving this requirement. An interim requirement of screening 50 percent of cargo transported on passenger aircraft by February 2009 has been met.

- ❑ Certified Cargo Screening Program (CCSP). This program assists industry in meeting the 100 percent domestic cargo screening requirement by August 2010. It uses a supply chain approach to screen cargo from shippers, manufacturers, distribution centers, third-party logistics providers, indirect air carriers (IAC), and independent screening facilities.
- ❑ Narrow-body Screening Amendment. This amendment, requiring 100 percent screening of cargo transported on all narrow body passenger aircraft, has greatly increased air cargo security by protecting the vast majority of passengers on passenger aircraft. This requirement was implemented by a regulatory program amendment that took effect in October 2008.

- ❑ Indirect Air Carrier (IAC) Screening Technology Pilot. A screening technology pilot was implemented for certain high-volume IACs that are CCSP members. The pilot enhances capacity by providing guidance and transferring authority for private industry cargo screening, measures the effectiveness of select screening technologies on various commodity classes, and evaluates chain-of-custody procedures for screened cargo as it moves from the IAC to the air carrier.
- ❑ International Collaboration. Efforts to align activities with foreign partners will increase global air cargo security and reduce burdens on trade. Agreements with the European Community and the Quadrilateral Working Group (QUAD), composed of the United States, Canada, Australia, and European Union member states, facilitate the signatories' seeking common and practical solutions to air cargo screening. This harmonization will contribute greatly to achieving the 100 percent screening requirement of the 9/11 Act.

4.2 Mass Transit and Passenger Rail

The Nation's transit, commuter, and long-distance rail systems stand out among transportation modes because of their openness and the sheer volume of passengers carried on such systems across the country every day. The risk-reduction strategy for mass transit and passenger rail is based on following five guiding priorities:

- ❑ Expanding security partnerships,
- ❑ Building security force multipliers,
- ❑ Elevating security baselines,
- ❑ Leading information assurance, and
- ❑ Mitigating high consequence risk.

Over the past year, several new robust security initiatives were implemented and existing ones were greatly enhanced.

- ❑ Baseline Assessment for Security Enhancement (BASE) Program. The BASE program assesses the security posture of transit agencies in 17 Security and Emergency Management Action Items. The results of these assessments inform security priority, security enhancement program, and resource allocation decisions.
 - Mass Transit and Commuter Rail. The program is progressing towards the goal of completing assessments of the largest 100 mass transit agencies, which account for 80 percent of the total users of mass transit and passenger rail systems. In 2008, 85 BASE assessments were completed, covering 48 of the 50 largest mass transit and passenger rail agencies, 27 of the next 50 largest agencies, and 10 smaller agencies.
 - Bus. TSA assessed 29 bus-only systems. Results were used to identify areas for improvement and to develop security enhancement tools for smaller bus agencies.
- ❑ Security Training. TSA and its security partners developed and implemented the Mass Transit Security Training Program, coordinated through the Mass Transit Sector Coordinating Council (SCC) and the Transit Policing and Security Peer Advisory Group. The Program provides guidelines to mass transit and passenger rail agencies on the types of training to be provided, based on category of employee. Core training areas include

security awareness, behavior recognition, and immediate response to a threat or security incident.

- ❑ National Tunnel Security Initiative. The Interagency Tunnel Security Working Group identified, assessed, and prioritized risks to mass transit systems with underwater tunnels. The effort helps transit agencies to design and implement protective measures to deter and prevent attacks, and to develop blast mitigation and emergency response strategies. In 2008, the Tunnel Security Initiative prioritized risk mitigation projects (*e.g.* enhanced surveillance and intrusion detection capabilities and anomaly and explosives detection systems, dedicated anti-terrorism operational teams, expanded explosives detection canine patrols, anti-terrorism training, drills and exercises, and multi-media public awareness activities); designed recommended protective measures; and developed strategies to fund future technology research and development aimed at novel technical solutions.
- ❑ Information Sharing. To enhance intelligence sharing, a multi-faceted process was established to ensure timely notification of threats, incidents, and related security concerns. The Mass Transit Information Sharing Network brings together representatives from approximately 15 key offices within DHS and the Department of Transportation (DOT). The Network's primary mission is to enable informed decision-making on security measures and actions during periods of heightened threat or security incidents. In addition the Public Transit Information Sharing and Analysis Center communicates security-related information and advisories obtained through open and secure sources to over 400 public transit systems. It plays a vital role in facilitating communication and coordination of information related to terrorism.
- ❑ Security Standards Development. TSA and its Federal partners continue to work with the American Public Transportation Association Security Standards Policy and Planning Committee to develop best practices to enhance security in transit systems. This collaborative effort facilitates the development of consensus-based standards in the areas of infrastructure protection, emergency management, and risk assessment. TSA plans to provide the security practices derived from the BASE program to the appropriate working groups, to spur progress and expedite completion of industry security standards.

4.3 Freight Rail

The freight rail system's ability to move large volumes of material quickly makes it essential to our national defense and economic security. The security objectives for the freight rail mode are:

- ❑ Establishing performance-based security standards,
- ❑ Enhancing the security of hazardous material (HAZMAT) shipments,
- ❑ Enhancing emergency preparedness, response, and recovery capabilities, and
- ❑ Enhancing detection and deterrence capabilities for critical infrastructure.

Over the past year several new robust security initiatives were implemented and existing ones were greatly enhanced.

- ❑ Toxic Inhalation Hazard (TIH) Risk Reduction Program. This program focuses on reducing risk by minimizing the time shipments of commodities that pose a toxic inhalation hazard spend in High Threat Urban Areas (HTUA). An industry baseline captures the level of risk associated with the transportation of TIH shipments and allows

for objective measurement of risk reduction by operator. Using this assessment, a 60 percent risk reduction had been achieved through 2008. This risk reduction was achieved without rules, regulations or security directives, but rather through the cooperative efforts of railroad carriers.

- ❑ Rail Transportation Security Final Rule (73 FR 72130). Published on November 26, 2008, the Rail Security Final Rule enhances security of freight and passenger rail by requiring railroad operators to designate security coordinators and report significant security concerns. The rule also codifies TSA's broad inspection authorities. It specifically addresses rail transportation of Security-Sensitive Materials (SSM), including TIH materials, by establishing secure chain-of-custody requirements for freight railroad carriers, rail HAZMAT shippers, and rail HAZMAT receivers located in a HTUA. When requested by the Federal Government, covered entities are also required to report on the location of individual rail cars containing rail SSM within 5 minutes and the locations of all cars containing rail SSM within 30 minutes.
- ❑ Rail Corridor Assessments. DHS and DOT continue to assess the vulnerabilities of high-population areas where TIH is moved by rail in significant quantities. Teams comprised of subject matter experts (SMEs) from TSA, the Federal Railroad Administration (FRA), the Pipeline and Hazardous Materials Safety Administration (PHMSA), DHS, affected railroads, and State and local homeland security officials conduct the assessments, which aid in identifying areas of high consequence and vulnerability. The scope of the assessments was recently expanded to include all 60 designated HTUAs. Surface Transportation Security Inspectors (TSIs) are being utilized to conduct these additional assessments. Through 2008, the following assessments have been completed: Philadelphia, Washington, D.C., Northern New Jersey, Cleveland, New Orleans, Houston, Los Angeles, Chicago, and Buffalo, New York.
- ❑ Rail Routing Final Rule (73 FR 7218). Published on November 26, 2008, the PHMSA rule requires rail carriers to annually collect data on the movements of SSM (such as TIH), analyze safety and security risks along the routes these materials are transported as well as all practicable alternative routes over which the carrier has authority to operate, and to select the route posing the least overall safety and security risk. FRA enforces the rule and may, in consultation with PHMSA, TSA, and the Surface Transportation Board, require a carrier to use an alternative route to the route selected by the carrier if FRA determines that the carrier's route selection documentation and underlying analysis are deficient and fail to establish that the route chosen by the carrier poses the least overall safety and security risk.
- ❑ Corporate Security Reviews (CSRs). The CSR Program examines freight railroad carriers' security plans for sufficiency by focusing on the following areas: physical security, communication, cyber security, hazardous materials security, and training. Following this evaluation, a determination is made of the degree to which mitigation measures are implemented throughout the company and recommendations are provided for additional mitigation measures. This "instructive" review of a company's security plan and procedures provides the government with a general understanding of each freight railroad's ability to protect its critical assets and its methods for protecting HAZMAT under its control. Recommendations of specific mitigation strategies are tied to identified vulnerabilities and are discussed with company officials. CSRs for all seven

Class I railroads were completed in 2007. In 2008, TSA completed 38 CSRs on short line and regional railroad carriers.

- ❑ Tank Car Threat Assessments. As required by Section 1519(a) of the 9/11 Act, 6 U.S.C. § 1169, TSA completed a project to identify, define, and prioritize threat scenarios for rail tank cars containing TIH materials, to evaluate the likely methods of attack to breach a TIH tank car, and to define the types and amounts of explosives and weaponry that might be used against a TIH tank car. The tank car threat analysis was conducted by an interagency technical team consisting of representatives from TSA, the Department of Defense (DoD), the Federal Bureau of Investigation, and DOT. The technical team determined the five weapons most likely to be used in an attack on a TIH tank car and evaluated the efficacy and limitations of each in a classified report.

4.4 Highway and Motor Carrier

The diversity of the trucking industry poses significant challenges to integrate security effectively in both large, complex trucking operations and smaller owner/operator businesses. The security objectives for the highway and motor carrier mode are:

- ❑ Standardizing risk assessment and risk mitigation approaches,
- ❑ Establishing performance-based security guidelines,
- ❑ Enhancing owner/operator awareness and training,
- ❑ Expanding development and adoption of security technology,
- ❑ Enhancing driver threat assessments and credentialing, and
- ❑ Expanding existing HAZMAT security requirements.

TSA has continued to develop and bolster security initiatives in the Highway and Motor Carrier mode throughout 2008 to address each of these objectives.

- ❑ Security-Sensitive HAZMAT Security Action Items. On June 26, 2008, Security Action Items (SAIs), which are voluntary measures provided to carriers for consideration during their security plan development process, were released to HAZMAT motor carriers. The SAIs are divided into four categories: 1) general security, 2) personnel security, 3) unauthorized access, and 4) en-route security. Action items include 23 voluntary practices for implementation by motor carriers transporting certain HAZMAT that are divided into two tiers (Tier 1 and Tier 2 SSM). The SAIs are implemented according to the risks associated with each Tier of SSM. TSA plans to incorporate the SAIs into a regulatory program in the future.
- ❑ Background Checks. All commercial vehicle drivers who transport HAZMAT must have a Hazardous Materials Endorsement (HME), which requires a Security Threat Assessment (STA). The STA is conducted under the direction of the Office of Transportation Threat Assessment and Credentialing (TTAC) in accordance with regulations in 49 CFR, Part 1572. To date, approximately 1.4 million of the estimated 2.7 million licensees who had HMEs prior to this regulatory change have completed STAs. Additionally, approximately 101,000 drivers have completed this requirement through the Transportation Workers Identification Credential (TWIC) background check process.

- ❑ Strategic Plan for High-Risk Bridge and Tunnel Hardening. A National Strategy for Highway Bridge Security, which includes establishing a security enhancement fund exclusively available for use on highway structures, is being finalized. Additionally, work is being done with State authorities in Maryland and Virginia to train bridge inspectors in the recognition of security threats during bridge inspections, and DHS will be awarding a contract to complete in-depth security assessments of the Nation's top 58 critical highway infrastructures.
- ❑ Training and Security Plan Regulations for Trucks and Commercial Buses. As required under Sections 1531 and 1534 of the 9/11 Act, 6 U.S.C. §§ 1181 and 1184, regulations are being drafted to require security assessments and plans, as well as training programs, for motor coaches operators. Similar requirements are being considered for a subset of the trucking industry (to include at a minimum those operators who carry SSM as defined in the SAI released in June 2008).
- ❑ Grants. The 2008 Intercity Bus Security Grant Program (IBSGP) provided over \$11 million to owners/operators of fixed route intercity buses and charter services using over-the-road buses. In addition, the Truck Security Grant Program provided over \$15 million to establish and maintain a 24/7 call center for anti-terrorism and security awareness program, maintain the Highway Information Sharing and Analysis Center, update and maintain the anti-terrorism and security awareness training program, and develop methodologies to identify and recruit highway professionals to actively participate in an anti-terrorism and security awareness program.
- ❑ CSRs. CSRs were conducted on 27 motor carriers, 4 motorcoach operators, 4 school transportation operators, and 4 State transportation departments (including three for follow-up reviews). These reviews allow us to assess the industry's level of security planning and implementation, build relationships, and share effective security practices.
- ❑ Memorandum of Understanding. As required by Section 1541 of the 9/11 Act, DHS, acting through TSA, and DOT, acting through the Federal Motor Carrier Safety Administration, signed an Annex to the DHS/DOT Memorandum of Understanding in October 2008. This document defines the specific roles and delineates the responsibilities between the two agencies to address motor carrier transportation security matters, including over-the-road bus security matters and processes the agencies will follow to promote communications, efficiency, and non-duplication of effort.

4.5 Maritime

The National Strategy for Maritime Security, its eight subordinate security plans, and the Maritime Modal Security Plan identify three major security priorities to reduce security risks in the mode:

- ❑ Protecting, preventing, and deterring acts of terrorism against, or involving the use of, the maritime transportation systems;
- ❑ Enhancing the resiliency of the transportation system; and
- ❑ Maximizing the cost-effectiveness of the limited resources of the maritime transportation systems sector.

TSA's maritime security activities in support of the U. S. Coast Guard's (USCG) mission lead in maritime security are listed below.

- ❑ Transportation Worker Identification Credential (TWIC). TWIC is a common identification credential for all personnel requiring unescorted access to secure areas of maritime facilities and vessels, and all mariners holding USCG-issued credentials. Individuals who meet TWIC eligibility requirements will be issued a tamper-resistant credential containing the worker's biometric to allow for a positive link between the card and the individual. TWIC was first deployed in October 2007 at the Port of Wilmington, Delaware. To date, enrollment sites have been established at over 150 locations nationwide. To complement fixed enrollment centers, nearly 400 mobile enrollment locations have been deployed to address the needs of stakeholders. As of December 3, 2008, more than 703,000 workers have successfully enrolled in the TWIC program and more than 625,000 workers have completed the background check process and were issued TWIC cards. These figures are tracked and updated weekly. Additionally, more than 470,000 workers have activated their cards. The USCG initiated a second TWIC rulemaking to establish requirements for biometric readers.
- ❑ DHS Infrastructure Protection Port Security and Transit Ferry Security Grant Program. 2008 grant funding totaled \$400 million, of which approximately \$5 million was designated specifically for passenger/vehicle ferries. In total, approximately \$1.5 billion has been awarded in eight rounds of port security grants. TSA contributed operational subject matter expertise for both port and transit ferry systems, in coordination with the USCG, DOT's Maritime Administration, and the Federal Emergency Management Agency (FEMA) in setting policy and award priorities, and recommending award distribution.
- ❑ Explosives Detection on Ferry Operations and Cruise Ship Terminals. The Security Enhancement and Capabilities Augmentation Program (SEACAP) enhances DHS's capability to deter, detect, and prevent explosives from being introduced as weapons on ferries and in cruise line terminals. In 2008, TSA tested the Transportable Radiation Monitoring System at the Galveston-Port Bolivar ferry in Galveston, Texas, as well as the Z-Portal vehicle x-ray screening system with the North Carolina Department of Transportation, Ferry Division. SEACAP operates in the Nation's top 25 Passenger Vessel Systems (Ferry and Cruise Ship Operations).
- ❑ Security Awareness Training. In 2008, TSA released a CD-ROM course entitled "Vehicle Borne Improvised Explosive Device/Improvised Explosive Device Recognition/Response for Passenger Vessels and Terminals." To date, TSA has distributed to passenger vessel and terminal operators approximately 2,800 copies of this training program. Additionally, in 2008, TSA hosted Maritime Explosives Security Seminars in the port areas of Seattle, Washington, and Boston, Massachusetts, that brought together more than 100 members of local and Federal agencies, bomb squads, first responders, and the maritime industry to discuss port and maritime security.

4.6 Pipeline

The Nation's pipeline industry has made good progress on assessing risks associated with its control centers, and in many cases, has established system redundancy. Operators have also taken

specific steps to harden facilities and increase visitor and vehicle monitoring, and have posted guards at critical facilities with higher threat levels to help deter a terrorist attack.

The risk reduction strategies for pipeline focus on:

- ❑ Developing a pipeline system-relative risk ranking and prioritization tool;
- ❑ Distributing baseline smart practices and security guidelines;
- ❑ Conducting pipeline international cross-border vulnerability assessments; and
- ❑ Improving relationships with government and private sector pipeline stakeholders using the Government Coordinating Council (GCC)/Sector Coordinating Council (SCC) framework, monthly stakeholder conference calls, and an annual International Pipeline Security Forum.

Over the past year, TSA implemented several new robust security initiatives and greatly enhanced existing ones.

- ❑ CSRs. The centerpiece of the pipeline security program is the CSR. Begun in 2003, CSRs are used to build relationships with pipeline operators, assess their corporate security plans and programs, and provide recommendations for improvement. The top 100 pipeline systems collectively transport 84 percent of the Nation's energy. CSRs were conducted on 12 of those systems in 2008, thereby completing reviews of the Nation's top 100 pipeline systems.
- ❑ Pipeline Employee Security Awareness Training. CSRs indicated shortcomings in many pipeline operators' security awareness training programs for frontline employees who are most likely to witness suspicious activity at field facilities. To address this issue, a training DVD was developed using DHS SMEs, but tailored specifically to an audience of pipeline operators. The training covers topics such as security measures, awareness of vulnerabilities, potential threats, and targeting.
- ❑ Cross-Border Pipeline Assessments. Recognizing the importance of securing the movement of energy resources between the United States and Canada, TSA participated in joint reviews of six of the largest cross-border pipeline systems. Teams of Canadian and U.S. government officials and other SMEs assessed control systems, infrastructure interdependencies, and assault planning processes to identify security gaps and provide options for consideration to enhance protective measures. Pipeline operators subsequently used the assessment results to target system improvements.
- ❑ Annual International Pipeline Security Forum. In conjunction with Natural Resources Canada, TSA has hosted an annual 2-day conference to enhance government and industry pipeline security domain awareness and provide opportunities for the discussion of major pipeline security issues. In 2008, more than 150 people attended the forum, including representatives and officials from the U.S. and Canadian governments, pipeline associations, U.S. and Canadian pipeline operators, and representatives from the security, intelligence, and law enforcement communities.
- ❑ Pipeline Security Guidelines. In 2002, DOT's Office of Pipeline Safety issued pipeline security guidelines to improve the security posture of the pipeline industry. CSRs of pipeline operators were conducted based on these guidelines. After the DOT guidelines were published, TSA was designated in the National Infrastructure Protection Plan

(NIPP) as the Sector Specific Agency responsible for pipeline security. TSA is in the process of updating these guidelines with input from DOT and the private industry. Furthermore, under the 9/11 Act, TSA is tasked with determining the need for pipeline security regulations, and the updated guidelines may form the basis for regulatory action in the future if that becomes necessary.

4.7 Intermodal Transportation Interconnectivity

The Nation's transportation system is widely distributed, yet highly interconnected. Programs and initiatives are designed to account for the intermodal nature of the transportation system, whereby an event in one mode can affect another, and prevention, protection, and recovery efforts can be helped or hindered by existing intermodal connectivity and actions. TSA works with its security partners and stakeholders to ensure coordination at these modal interfaces. Key examples of TSA's current programs are highlighted in the following sections.

- ❑ Bomb Squad Response in Transportation Systems Training. TSA conducted five sessions which provided advanced technical training to 25 public safety bomb squads, comprising approximately 170 personnel, on responding to improvised explosive devices and explosives incidents in the aviation environment. Two additional training courses were conducted for 11 public safety bomb squads (consisting of 65 personnel) responsible for responding in the mass transit environment.
- ❑ Expanding Use of Explosives Detection Canine Teams (EDCTs). In 2008, the National Explosives Detection Canine Team Program deployed approximately 400 canine teams to 76 airports to conduct random explosives detection screening of cargo being loaded on passenger aircraft. Twenty-five percent of a TSA-certified EDCT's time is dedicated to screening cargo and mail for explosives prior to being loaded on passenger aircraft or to related deterrent activities. In mass transit systems, 62 TSA-certified explosives detection canine teams have been deployed. Their mobility enables random and unpredictable operations throughout the transportation systems.
- ❑ Training and Exercise Program. The Intermodal Security Training and Exercise Program (I-STEP) facilitates training and exercise management in all transportation modes. It brings together Federal, State, and local governments, and private industries to develop and test clear and consistent training and exercise performance measures. In 2008, I-STEP supported over 12 exercises involving maritime, mass transit, freight rail, and motorcoach bus modes of transport.
- ❑ Visible Intermodal Prevention and Response (VIPR) Program. Specifically authorized by Section 1303 of the 9/11 Act, 6 U.S.C. § 1112, VIPR teams flexibly integrate multiple TSA assets, including Federal Air Marshals, TSIs, TSOs, canine teams, Explosives Security Specialists, and advanced screening technology to augment the security in any mode of transportation. VIPR team personnel operate in a discreet manner, utilizing behavioral detection, surveillance detection, and counter surveillance activities. TSA has independently supported and partnered with other DHS agencies to conduct VIPR operations. In 2008, over 800 VIPR operations were deployed across the transportation sector to augment State and local security and law enforcement resources.

5. Research, Engineering, and Development Activities Related to Transportation Security

TSA works with its Federal, State, and local security partners and private sector stakeholders to address national Research and Development (R&D) initiatives in support of the NIPP/Transportation Systems Sector Specific Plan and the National Critical Infrastructure Protection R&D Plan. Working groups coordinate common requirements and intermodal needs among all partners and stakeholders along with other sectors that either influence or are influenced by transportation. Much of the progress of modal R&D initiatives is reflected in the prior modal sections. However, the following is a summary of key progress points for 2008.

5.1 Screening and Inspection - Passengers

- ❑ Checkpoint Evolution. This initiative improves passenger security systems through enhancing detection capability by reshaping the checkpoint environment. Checkpoint Evolution includes three strategic initiatives: 1) improve detection capability; 2) enhance behavior detection capability; and 3) establish partnerships to expand the security screening process throughout the passenger journey. In April 2008, TSA began its first integration pilot at Baltimore-Washington International Thurgood Marshall Airport (BWI). This pilot combines several programs from the explosives detection and behavior detection initiatives and is designed to provide a layered defense that extends beyond the checkpoint and into public spaces. The BWI checkpoint integrated a new layout, emerging technologies, and environmental elements, all designed to increase explosives detection, aid passenger flow, and provide an effective platform for behavior detection.
- ❑ Advanced Technology (AT) X-Ray. AT refers to the next generation of threat image projection-capable x-ray equipment that examines dimensions and densities of objects within a carry-on bag and provides dual images to TSOs for enhanced threat identification. TSA deployed approximately 500 AT units to Category X and I airports in 2008. TSA is working with the AT vendors to develop liquid threat detection capability that will potentially eliminate the liquid restrictions at checkpoints. Vendors have been developing liquid threat detection software that is currently being tested in a government explosives laboratory and in pilot mode at certain airports. In parallel, TSA is conducting a solicitation for the next generation of AT systems to enhance detection capability and improve performance.
- ❑ Bottled Liquids Scanners (BLS). The BLS is a hand-held or bench-top device with the capability to discriminate between liquid explosives or flammable liquids and common, benign liquids carried by passengers. TSA has deployed approximately 400 BLS systems designed to detect liquid threats emitted from liquid containers. TSA is in the process of procuring the next generation of BLS systems that will have greater threat recognition capability, eliminate the need to open bottles, and reduce the cost of operational consumables.
- ❑ Advanced Imaging Technology. This technology generates high-resolution images that allow TSOs to conduct secondary screening of passengers and inspect for all types of concealed weapons (metal and non-metal) in place of a traditional alarm resolution techniques (i.e. metal detection wand inspection and physical pat-down). TSA has

deployed approximately 50 systems. Passenger acceptance rating for millimeter wave and backscatter technology continues to be approximately 93 percent. TSA is conducting a number of pilots to improve throughput and communication efficiencies.

5.2 Screening and Inspection – Checked Baggage

- ❑ Passenger Volume. In the near-term (1 – 3 years), TSA will develop technologies to support variable passenger volumes at the Nation’s airports. Using the *Planning Guidelines and Design Standards for Checked Baggage Inspection Systems* published October 10, 2008, TSA is supporting the development and deployment of reduced-size medium-speed and high-speed checked baggage screening systems.
- ❑ Threat Detection. In the longer term (3 – 6 years), the Manhattan II program is focused on activities to develop next-generation explosive detection systems, and aims to develop and optimize threat-specific detection algorithms, and investigate and evaluate innovative ways to apply these algorithms to baggage screening.

5.3 Screening and Inspection – Cargo

- ❑ Explosives Detection. Numerous cargo screening improvement initiatives were developed to evaluate technologies to detect multiple types of explosives across a range of commodity classes. This includes the evaluation of unique scanning technologies for pallets and containers, the continued testing of Hardened Unit Load Device equipment designed to withstand explosive blasts, and additional studies of trace sensors to better detect explosive particles and vapor signatures.
- ❑ CCSP. A program designed to enable vetted, validated, and certified supply chain facilities to screen cargo before it is consolidated and delivered to the transport carriers is being tested.

5.4 Infrastructure and Conveyance Protection

5.4.1 Infrastructure Protection

- ❑ Rapid Response. TSA continued to investigate using robots and a highly portable utility rail car to assist first responders during incidents in tunnels and other hazardous environments. TSA also participated in joint field tests on rapid response to extreme events in tunnels, bridge and tunnel blast modeling and simulation, and the construction of a tunnel test track to enhance the evaluation of potential rail security threats.
- ❑ Intelligent Video and Virtual Fence for Infrastructure Protection. Test beds were established, and several intelligent video, video indexing and extraction to handheld devices, and virtual fence systems were evaluated. Projects are currently underway at Amtrak 30th Street Station in Philadelphia, Pennsylvania; the Port-Authority Trans-Hudson subway system in New York and New Jersey; and the St. Paul’s Avenue rail yards in Jersey City, New Jersey.
- ❑ TWIC Access Control. With the USCG, TSA has initiated pilot programs to test TWIC access control technologies in real-world marine environments.

5.4.2 Conveyance Protection

- ❑ Remote Disabling Systems. Field evaluations of remote disabling systems on buses were conducted in San Diego, with tests of ability to disable and stop diesel locomotives planned in the New York City area in 2009.
- ❑ Next Generation Rail Tank Car. Research on the Next Generation Rail Tank Car project, done jointly with the FRA and industry, continued with construction and testing of a prototype planned for 2009.

5.4.3 Improved Materials and Methods of New/Existing Structures

- ❑ Advanced Materials. TSA is working with the DHS Directorate for Science and Technology (S&T), academia, and private industry to explore advanced materials solutions such as nanotechnology, self-healing structures, and blast-absorbing materials to provide practical solutions for existing transportation structures. Initiatives include a “tunnel plug” or system that can seal breaks or hold back pressure from a break, paint that can detect and repair cracks in surface, and advances in steel and reinforced concrete for bridges and other structures.
- ❑ Building Security Integration. TSA continues to work closely with airport and industry designers and engineers, through the Airport Peer Review Group, to address integrating security into new and existing facility construction programs.
- ❑ Enabling or Complementary Technologies and Capabilities. TSA supports developing technologies intended to augment human performance. Pilot programs include passenger behavior assessment, suspicious behavior detection, voice stress analysis, and intelligent video technology.

6. Cooperative Efforts with Domestic and Foreign Security Partners

The need for public-private cooperation is crucial due to the wide spectrum of entities that own and operate transportation systems. Effective cooperation takes into account the expertise, and operational and economic concerns of all interested parties when developing security programs.

6.1 Other U.S. Departments, Agencies, Instrumentalities and State and Local Authorities

- ❑ Transportation Sector Government Coordinating Council (GCC)/Sector Coordinating Council (SCC). Significant progress has been made in building public-private partnerships to improve cooperation among stakeholders and partners. The GCCs and SCCs, as part of the Critical Infrastructure Protection Advisory Committee, coordinate security initiatives across the transportation sector and establish an institutionalized process for the private sector to participate in programmatic planning, strategy, policy, implementation, and joint monitoring of progress of transportation security initiatives.
- ❑ National Capital Region Coordination Center (NCRCC). The interagency NCRCC, co-located with TSA’s Transportation Security Operations Center, is staffed 24/7 by TSA, Federal Aviation Administration, DoD, Customs and Border Protection, USCG, United

States Secret Service, and the U.S. Capitol Police. Combined with other agencies that provide staffing as required, the NCRCC provides a coordinated response to any potential threats in the National Capital Region. In addition, the NCRCC enhances coordination for DoD and DHS aircraft performing aerial interdiction of tracks of interest flying in the Air Defense Identification Zone or other restricted airspace in the National Capital Region without authorization.

6.2 Foreign Transportation and Security Authorities

- ❑ Transportation Security Administration Representatives (TSAR). A cadre of 22 TSARs in 19 locations worldwide provided diplomatic liaison to coordinate, align, and ensure consistency between security requirements of the United States and those of foreign governments. These representatives also serve as principal advisors on transportation security affairs to U.S. Ambassadors and embassy officials. TSARs continually interact with individual partners on a bilateral and regional basis to improve compliance with U.S. and international standards. In 2008, TSA received approval to establish new TSAR positions in Amman, Jordan; Ottawa, Canada; New Delhi, India; Warsaw, Poland; and Berlin, Germany.
- ❑ Transportation Security Specialists (TSS). TSA's TSSs assess international airports for compliance with the Standards and Recommended Practices established by the International Civil Aviation Organization (ICAO). In 2008, over 140 airports were assessed, including those: served by U.S. air carriers; from which a foreign air carrier serves the United States; that pose a high risk to international air travel; and others as determined by the Secretary of DHS.
- ❑ International Air Carrier Program. One hundred sixty foreign passenger air carriers and 42 foreign all-cargo carriers operate to and from the United States. Six International Industry Representatives (IIR) in four locations worldwide liaise with international air carriers and international airline associations to provide regulatory guidance, ensure compliance with U.S. regulations, and promote positive government-industry relations. IIRs work with new start-up passenger and all-cargo air carriers to ensure compliance with TSA regulatory requirements. IIRs also receive and coordinate the sharing of aviation security requirements, intelligence, incidents and threat information.
- ❑ International Working Group on Land Transport Security. TSA has historically worked with the European Union, the Group of Eight (G8), Japan, the United Kingdom, Canada, and Mexico to discuss issues related to rail security. The first meeting of the International Working Group on Land Transport Security, which the United States hosted and chaired, was held in San Francisco, California, in November 2008. Over 20 transportation security officials from 12 countries, the European Commission, and the International Union of Railways gathered to discuss future cooperation, information sharing, research and development, emerging threats to mass transit security, and more.
- ❑ G8 Transportation Security Subgroup (TSSG). TSA is the lead U.S. agency for the TSSG, one of seven subgroups that convene concurrently during the G8 meetings. Since its creation as a formal subgroup, the TSSG has compiled and shared best practices and recommendations that have strengthened transportation security within the G8 nations and globally. Since 2002, G8 transportation security work has resulted in over 20

guidance documents exported to international organizations such as the ICAO, International Air Transport Association, International Federation of Airline Pilots' Associations, International Maritime Organization, and World Customs Organization. Through outreach programs and projects passed to ICAO, for example, TSSG products have been used to guide security practices in the international aviation sector by strengthening flight deck security, proposing more effective screening methods for passengers and baggage, and developing a checklist to address MANPADS. In 2008, the TSSG completed four projects dealing with future threats to aviation security, behavior observation techniques, screening methods for passengers and baggage and pipeline security.

- ❑ QUAD. This working group provides opportunities for the United States, the European Union, Australia, and Canada to discuss important transportation security issues and develop high-level responses to shape national and international security approaches or policy. This collaboration, drawing on informed best practice solutions, results in frameworks and principles that can be used in the development of more detailed national or international mitigation strategies. The QUAD increased information sharing by forming SME working groups on Liquids, Aerosols, and Gels (LAGs), GA, and Air Cargo. The LAGs group is currently working to develop common standards for LAGs screening technology and synchronize security measures. The QUAD developed and presented a paper to ICAO recommending a revised Prohibited Items List for aviation security that would better align global aviation security requirements. This paper was subsequently approved by ICAO and disseminated to ICAO member States.
- ❑ Asia-Pacific Economic Cooperation (APEC). TSA plays a leading role in two APEC sub-groups: the Counter Terrorism Task Force and the Transportation Working Group's Aviation Security Experts Group. Supporting the U.S. lead agency, the Department of State, TSA has promoted several new initiatives that include an aviation point-of-contact network, a passenger baggage screening practices paper, an air cargo workshop, and information sharing on capacity-building initiatives underway in the APEC region. Understanding the modalities and complexities of the APEC working groups has been a challenge that may be overcome by a TSA-led initiative to convene regularly an informal "strategy core group" of like-minded nations. The purpose of the core group is to support subgroup chairs in coordinating and completing projects in a timely manner and setting current and future priorities for the group.
- ❑ ICAO. TSA works closely with ICAO to strengthen aviation security standards and to encourage compliance with and coordination of those standards throughout the international aviation system. TSA actively participates in ICAO's Aviation Security Panel of Experts, which is the ICAO body responsible for promulgating international security standards; chairs the panel's New and Emerging Threats Working Group; and has two individuals assigned to ICAO's aviation security panel. TSA also works multilaterally with States through regional and international aviation security organizations, such as the European Civil Aviation Conference, the Latin American Civil Aviation Commission, the African Civil Aviation Commission, and other organizations. ICAO's Universal Security Audit Program contributes directly to U.S. homeland security by ensuring that each of ICAO's 190 member states undergo security audits and comply with international aviation security standards.

7. Budget, Staffing and Grants

7.1 An Accounting of DHS Personnel Working on Transportation Security

The 9/11 Act requires an accounting of personnel working on transportation security by mode. Table 1 indicates the number of Federal personnel designated for work (including part-time work) on transportation security issues in the various transportation modes as of September 30, 2008. DHS does not currently have procedures in place to collect similar information for contract personnel. The USCG figures separately account for civilian and military personnel. Employees designated for work on multiple modes or in indirect support were classified as “other.” Personnel were determined to be “working on transportation security” if they devoted more than 25 percent of their working hours in direct support of a transportation security function or more than 75 percent of their working hours in *indirect* support of a transportation security function (such as personnel, acquisition, finance, or administrative functions).

Table 1: DHS Personnel Working in Transportation Security

Mode	DHS HQ	TSA	USCG	CBP	FEMA	Total
Aviation	0	56,277	0	0	0	56,277
Maritime	0	17	AD Military: 8,686 Selected Reservists: 1,696	0	0	Total Military: 10,382
			Fed Civilian: 1,577	0	6	Fed Civilian: 1,600
Freight Rail	0	17	0	0	1	18
Highway	0	19	0	0	3	22
Mass Transit	0	19	0	0	4	23
Pipeline	0	12	0	0	0	12
Other (Multiple Modes / Indirect Support)	9	1,734	0	0	2	1,745
Total	9	58,095	Military: 10,382 Fed Civilian: 1,577	0	16	Military: 10,382 Fed Civilian: 59,697

Table 2 accounts for turnover among senior staff of DHS (and any component agencies) working on transportation security issues, including program managers responsible for transportation security programs, as well as their immediate supervisors and other superiors, up to and including Assistant Secretaries or Under Secretaries, during FY 2008. Senior staff means those permanently appointed to leadership positions for major organizational elements at or above GS-13, I-band, or the military grade of O-4.

Table 2: Turnover in Senior DHS Staff Working on Transportation Security

	DHS HQ	TSA (I-band and above)	USCG (GS-13 and 0-4 and above)	CBP	FEMA	Total
Average Number of Transportation Security Senior Staff personnel onboard in FY 2007	9	7,829	Military: 529 Civilian: 363	0	0	Military: 529 Civilian: 8,201
Number of Senior Staff personnel who left those positions during FY 2007	0	568	Military: 167 Civilian: 27	0	0	Military: 167 Civilian: 595
Turnover rate = # of Senior Staff personnel who left / average onboard count (in %)	0	7.25%	Military: 31.6% Civilian: 7.5%	N/A	N/A	Military: 31.6% Civilian: 7.3%

The computation of senior staff turnover was determined by:

1. **Average Number of Senior Staff.** Derived from the sum of senior staff personnel on board at the beginning of the fiscal year (10/1/2007) and the number on board at the end of the fiscal year (9/30/2008) divided by two. Where this method did not yield representative results, agencies were permitted to use an alternative method, for example when the senior staff population varied significantly throughout the year.
2. **Number of Senior Staff Personnel Who Left.** Simple accounting of the number of senior staff that left positions during FY 2008.
3. **Turnover Rate.** Derived by dividing the number of personnel who left by the average onboard count. The accounting processes used to gather the required information are newly developed and the data has not been validated. DHS intends to refine the protocols and document the process to assure uniformity in data collection among its offices and agencies in FY 2009.

7.2 Accounting of Funding in the President's Budget for Transportation Security

DHS is developing accounting protocols to comply with the 9/11 Act's budgetary information requirement. These procedures will provide guidance to DHS agencies regarding the modal breakdown of funds that were budgeted and expended under broadly defined accounts, such as the surface transportation security program and the transportation support program accounts. The guidance will also address how the USCG will determine the portion of its program accounts that can be accounted for under its transportation security responsibilities. Likewise, the guidance will assist other DHS offices and agencies with cross-modal responsibilities in apportioning their transportation security funds to the different modes. The next annual progress report will provide data for FY 2009.

7.3 Reducing Risks through Security Grants

The 9/11 Act requires an accounting of all grants for transportation security awarded by the Secretary, and a description of how the grants accomplish the Department's goals. The program accomplishments are described below. The subsections below show the distribution of the grant awards for FY 2008.

7.3.1 Transit Security Grant Program (TSGP):

The TSGP provides funding to transit agencies, ferry systems, Amtrak, and transit security providers to enhance regional security and mitigate risk. In 2008, DHS continued the process of entering into cooperative agreements in the highest risk regions. This method for establishing grant awards provided the ability to align grant funds to the overall regional security programs developed collaboratively with the Regional Transit Security Working Groups. The 2008 TSGP eligibility list included law enforcement agencies that provide dedicated transit security support as sub-grantees of the transit agency to which they provide service. Certain personnel costs associated with operational activities such as canine teams, mobile screening teams, and VIPR teams, were also authorized for grant support. For the first time, in 2008, allocations published in the grant guidance represented target amounts so that funding could be shifted among the Tier I regions and between tiers, as DHS deemed appropriate, to maximize the security benefit to the Nation based on the overall quality and effectiveness of the projects submitted. Per the 9/11 Act, transit agencies were required to have a current vulnerability assessment and security plan in order to be eligible for grant funding. Agencies that did not have an assessment and/or plan were only allowed to request funding for the development of the assessment/plan.

The funding priorities for the 2008 TSGP were organized into Project Effectiveness Groups and prioritized as follows:

- ☐ Training, Operational Deterrence, Drills, Public Awareness Activities, Security Planning,
- ☐ Multi-User High-Density Key Infrastructure Protection,
- ☐ Single-User High-Density Key Infrastructure Protection,
- ☐ Key Operating Asset Protection

In 2008, DHS also introduced the Freight Rail Security Grant Program. Funding was carved out of the overall appropriation for transit security to provide support for Class I, II, and III railroad carriers to conduct vulnerability assessments, develop security plans, and to train frontline employees in security awareness.

Table 3: Transit Security Grant Program Distributions

Tier/Agency	2008 Target Allocation	2008 Award
Atlanta Region	\$6,399,055	\$6,399,055
Boston Region	\$29,259,896	\$29,259,896
Chicago Region	\$24,856,829	\$25,997,331
Los Angeles Region	\$13,333,678	\$13,511,417
National Capital Region	\$38,080,340	\$38,371,355
New York City Region	\$153,256,664	\$175,380,995
Philadelphia Region	\$18,553,816	\$18,888,660
San Francisco Bay Area	\$28,259,722	\$25,433,749
Amtrak	\$25,000,000	\$25,000,000
Tier II	\$36,600,000	\$22,866,113
FRSGP	\$15,000,000	\$7,491,429
TOTAL	\$388,600,000	\$388,600,000

7.3.2 Intercity Bus Security Grant Program (IBSGP)

The IBSGP provided grants to operators of fixed route intercity and charter bus services. In 2008, eligible operators were divided into two tiers, with the largest operators in Tier I and remaining eligible operators in Tier II. As with the TSGP, the awards made to the Tier I bus operators were in the form of cooperative agreements, allowing TSA more interaction and dialogue with the operators throughout the process.

The funding priorities for the 2008 IBSGP followed the allowable uses of funds outlined in the 9/11 Act, and were prioritized as follows:

- ☐ Development of assessments or security plans;
- ☐ Operating and capital costs associated with over-the-road bus security awareness, preparedness, and response training, including training for front-line employees for potential security threats and conditions;
- ☐ Live or simulated exercises for the purpose of assessing and improving the capabilities of entities to prevent, prepare for, mitigate, respond to, and recover from acts of terrorism;
- ☐ Public awareness campaigns for enhanced over-the-road bus security;
- ☐ Modifying over-the-road buses to increase their security;
- ☐ Installing cameras and video surveillance equipment on over-the-road buses and at terminals, garages, and over-the-road bus facilities;
- ☐ Constructing and modifying terminals, garages, and facilities, including terminals and other over-the-road bus facilities owned by State or local governments, to increase their security;
- ☐ Establishing and improving an emergency communications system linking drivers and over-the-road buses to the recipient's operations center or linking the operations center to law enforcement and emergency personnel;

- ☐ Implementing and operating passenger screening programs for weapons and explosives;
- ☐ Protecting or isolating the driver of an over-the-road bus;
- ☐ Chemical, biological, radiological, or explosives detection, including canine patrols for such detection;
- ☐ Acquiring, upgrading, installing, or operating equipment, software, or accessorial services for collection, storage, or exchange of passenger and driver information through ticketing systems or other means and for information links with government agencies, for security purposes;
- ☐ Overtime reimbursement, including reimbursement of State, local, and tribal governments for costs, for enhanced security personnel assigned to duties related to over-the-road bus security during periods of Orange or Red Alert levels or National Special Security Events.

Table 4: Intercity Bus Security Grant Program

Company	2008 Award
Academy Express, LLC.	\$836,953
Coach America (CUSA, LLC)	\$450,906
Coach USA Inc.	\$739,350
Greyhound	\$3,459,500
Peter Pan	\$674,865
Tier II Companies	\$5,010,676
TOTAL	\$11,172,250

7.3.3 Trucking Security Grant Program (TSP)

The Trucking Security Grant Program provided funding to assist highway professionals and operating entities in obtaining the skills and abilities required to support national goals and priorities. Grants had previously been awarded directly to the American Trucking Associations, but were directed by Congress to be competed for 2008. This resulted in an award and grant distribution to the HMS Company for **\$15,544,000**.

The funding priorities for the 2008 TSP were:

- ☐ Participant identification and recruitment,
- ☐ Planning,
- ☐ Training,
- ☐ Communications, and
- ☐ Information analysis and distribution.

7.3.4 Port Security Grant Program (PSGP)

Seven port areas qualified for Tier I, or highest risk status, in 2008 and received a combined total of \$220.8 million, or roughly 57 percent of the amount funded through the PSGP. The remaining U.S. ports were included within three additional risk tiers. Grant funding priorities included training; exercises; activities to mitigate the risk of IEDs; employee credentials and access controls; assistance to ports in enhancing risk management capabilities; enhanced

domain awareness; and capabilities to prevent, detect, respond to, and recover from attacks involving IEDs and other non-conventional weapons. The PSGP also included a competitive ferry component, which provided funding to five systems.

Table 5: PSGP Awards

Tier	Port	FY 2008 Total Award*
I	New York-New Jersey	\$45,503,961
I	New Orleans	\$30,845,686
I	Houston-Galveston	\$32,289,262
I	Los Angeles-Long Beach	\$38,156,658
I	Puget Sound (Seattle-Tacoma)	\$27,263,241
I	Delaware Bay (Philadelphia, Wilmington, DL & Southern NJ)	\$20,041,972
I	San Francisco Bay	\$26,772,907
II	All	\$138,116,776
III	All	\$17,289,869
All Other	All	\$9,877,383
Ferry	All	\$2,442,285
	Total	\$388,600,000

*Rounded to the nearest hundred thousand dollars.

7.3.4 Buffer Zone Protection Program (BZPP)

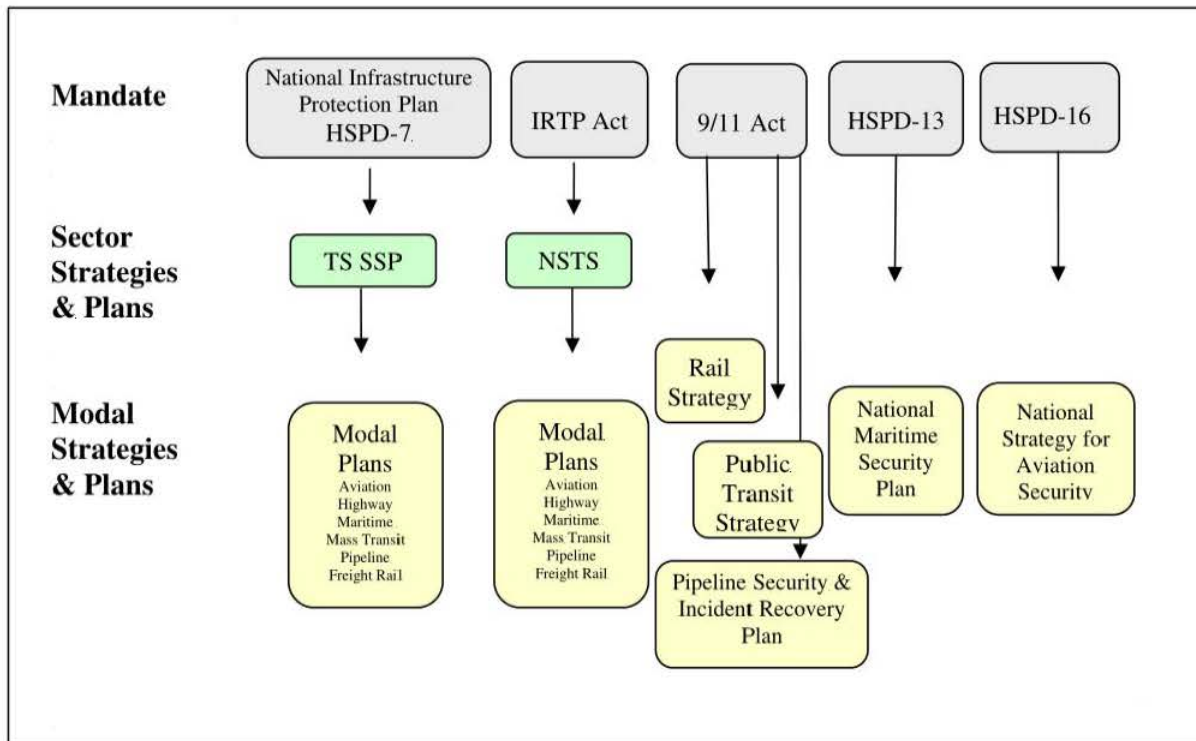
The BZPP is a DHS-administered, targeted infrastructure protection grant program for local law enforcement (LLE) focused on identifying and mitigating vulnerabilities at the highest-risk critical infrastructure sites and providing funding to LLE to address gaps and enhance security capabilities. The total grant distribution for FY 2008 for the Transportation Sector was \$3,582,000.00. The funding priorities within the Transportation Sector for the 2008 BZPP were bridges and rail yards.

8. Conclusion/DHS Action Plan

As mentioned in previous reports, TSA and the Transportation Systems Sector must conform to several strategic planning and reporting requirements issued by the administration and Congress. While each document has some unique content requirements, they essentially address the same threats and risks and express similar strategies and programs for securing the Sector. The overlapping sector strategic documents, the different planning cycles, and multiple annual reports create a difficult situation for government and private sector security partners. Since security planning is engaged through collaboration with stakeholders, the repetitive and redundant work associated with developing multiple similar planning documents creates costly inefficiencies that are detrimental to effective working relationships with security partners and stakeholders.

The diagram below provides a pictorial representation of the strategies and plans currently mandated. The divergent planning cycles may result in strategies and plans that, although current, may contain differences. Updates in one document simply may not be reflected in other documents on a different maintenance cycle. Clearly, good governance and responsible

management demand a more centralized planning regime for the Sector. TSA will strive to merge the strategies and reports to the greatest extent possible. TSA hopes to work with Congress to streamline these reporting requirements.



Appendices

Appendix (A) - 2008 Report on Enhanced Security Measures

I. INTRODUCTION

Section 109(a) of ATSA authorizes TSA to take certain actions in eight specific areas to enhance the security of transportation. Section 109(b) of ATSA requires that within six months of the Act's enactment, and annually thereafter, TSA transmit to Congress a report on its progress in evaluating and taking such actions, including any legislative recommendations that may be necessary for enhancing transportation security. This report is required annually until all specified actions are evaluated and implemented or TSA has decided not to pursue further action.

TSA evaluated and closed out actions under section 109(a)(1) (effective 911 emergency call capability for telephones serving passenger aircraft and trains) and (4) (alternative security procedures for safe medical product inspection) in the first report, and actions under section 109(a)(6) (whether to require all pilot licenses to incorporate a photograph of the license holder and appropriate biometric imprints) in the 2005 Annual Report.

This report covers Calendar Year 2008, January 1 through December 31, 2008, and describes actions taken by TSA and other agencies on the remaining five statutorily identified items.

II. STATUS OF TSA EVALUATIONS

Section 109(a)(2): Establish a uniform system of identification for all State and local law enforcement personnel for use in obtaining permission to carry weapons in aircraft cabins and in obtaining access to a secured area of an airport, if otherwise authorized to carry such weapons.

Discussion: The need for a Law Enforcement Officers (LEO) identification system for use in the aviation environment is well-recognized and has been the subject of detailed study by interagency working groups and the Aviation Security Advisory Committee. Reinforcing Section 109 of ATSA, Section 4011 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), P.L. 108-458, requires the establishment of a "law enforcement officer travel credential that incorporates biometric identifier technology and is applied uniformly across all Federal, State, local, tribal, and territorial government law enforcement agencies."

This issue was addressed at the four *State and Local Law Enforcement LEO Flying Armed Forums* hosted by TSA in March, April, June, and October of 2008. In attendance were representatives from various Federal, State, and local law enforcement agencies and several national professional organizations, including the International Association of Chiefs of Police, Major County Sheriffs' Association, Airport Law Enforcement Agencies Network, Personnel Security Working Group, and the Fraternal Order of Police.

The agreed upon solution was to replace the original letter of authority, signed by the LEO's authorizing official, confirming the need to travel armed and detailing the itinerary, required under 49 CFR § 1544.219, with a National Law Enforcement Telecommunications (NLETS) message conveying that information. The NLETS system is cost effective, and utilizes existing technology facilitating secure communication between all Federal, State, and local law enforcement agencies.

On November 15, 2008, TSA began transitioning to this solution by adding a requirement that the employing agency send an NLETS message in addition to the currently required original letter of authority. Once the NLETS message is received by TSA, a return message is sent to the employing agency, assigning a unique identifier for verification at the airport on the day of travel. The NLETS message, along with the original letter of authority, is retained until otherwise notified by TSA. Specific instructions on how to format and submit NLETS messages have been provided by TSA to all State and local law enforcement agencies. Eventually, use of the NLETS message, in lieu of the letter, will become mandatory.

This system provides a more secure means of confirming the identity of State and local LEOs, eliminates the potential for fraudulent or counterfeit authorizations, and ultimately restricts the ability of individuals to fly armed without authorization of their employing agency.

Status: *Closed.* The system is fully operational and continues to be updated with additional software enhancements.

Section 109(a)(3): Establish requirements to implement trusted passenger programs and use available technologies to expedite the security screening of passengers who participate in such programs, thereby allowing security-screening personnel to focus on those passengers who should be subject to more extensive screening.

Discussion: TSA developed Registered Traveler (RT) through a series of three pilots. The first, the RT Pilot Program, was a federally managed pilot conducted at five designated airports that established the use of biometrics in identity verification and determined baselines for public acceptance. The second, the Private Sector Known Traveler Pilot, tested the feasibility of implementing RT through a public/private partnership at a single airport. The third, the Registered Traveler Interoperability Pilot (RTIP), further tested and evaluated the trusted traveler passenger model and introduced interoperability among participating airports/air carriers and operated with larger populations.

In evaluating the RTIP, TSA concluded that: 1) current technology is insufficient to allow anyone to bypass the minimum screening procedures at airport security checkpoints; 2) an individual's successful completion of a TSA-conducted security threat assessment did not eliminate the possibility that the individual might initiate an action that threatens the lives of other passengers and that screening procedures should remain the same for all passengers; and 3) while effective identity verification is a critically important element in a multi-layered approach to aviation security, RT cannot currently function as a stand-alone security program.

Based on these conclusions, TSA published a notice on July 30, 2008, in the Federal Register announcing the conclusion of the RTIP and the decision to focus the government role in relation to RT on its identity verification benefits. The notice further reflected that although the private sector will have the primary role in RT, TSA will set security standards through amendments to Sponsoring Entities' security programs, continue to exercise oversight of the Sponsoring Entities to ensure compliance with established security standards, and continue its screening operations at the security checkpoint.

Status: *Closed.* No further action by the Federal Government is anticipated.

Section 109(a)(5): Provide for the use of technologies, including wireless and wire line data technologies, to enable the private and secure communication of threats to aid in the screening of passengers and other individuals on airport property who are identified on any State or Federal security-related database for the purpose of having an integrated response coordination of various authorized airport security forces.

Discussion: TSA actively pursues the use of technologies to improve communication regarding threats. Air carriers currently operate the Federal Government-mandated Computer-Assisted Passenger Prescreening System to identify passengers and their checked baggage for enhanced screening before those passengers are permitted to board commercial aircraft. Airlines also perform watch list matching of passenger data against the “no fly” and “selectee” portions of the consolidated terrorist watchlist (respectively, people who cannot fly and people who require additional scrutiny before they can fly because of suspected ties to terrorism) provided by TSA, and must alert TSA to potential hits. Section 4012 of IRTPA requires TSA to oversee the performance of such terrorist watch list checks. To meet this requirement, TSA is developing Secure Flight, an enhanced passenger prescreening program that will meet the Department’s goals of improving the security and safety of travelers on domestic and international flights, reducing passenger checkpoint screening time, and protecting privacy and civil liberties.

Under Secure Flight, TSA will compare limited passenger information submitted by aircraft operators to comprehensive watch lists maintained by the Federal Government in the effort to identify known and suspected terrorists, prevent known and suspected terrorists from boarding aircraft, facilitate legitimate passenger air travel, and protect individuals’ privacy. Secure Flight will match this limited passenger information for travelers on domestic or international flights arriving in, departing from, or over-flying the continental United States and for authorized non-traveling individuals (those requesting access to the sterile area of an airport). TSA continues to coordinate with the U.S. Customs and Border Protection (CBP) to implement the domestic matching program and will transition the international component in a unified and consistent manner to reduce public inconvenience and private sector operational and economic impacts.

Consolidating watch list checks within the Federal Government will allow TSA to automate most watch list comparisons and apply more consistent internal analytical procedures when automated resolution of potential matches is not possible. It is designed to help eliminate false positive watch list matching results that passengers experience under the existing system, help move passengers through airport screening checkpoints more quickly, reduce the number of individuals selected for secondary screening, and allow for more consistent response procedures at airports for those passengers identified as potential matches. Secure Flight differs from earlier proposed systems by eliminating the predictive “risk assessment” features and limiting the amount of passenger information it collects.

Status: *Active.* The program began parallel testing with volunteer aircraft operators in fall 2008 and completed this testing in December 2008. A phased implementation of the program began with these volunteer aircraft operators in early 2009, with other domestic aircraft operators switching over throughout the year. Full implementation of the program with all domestic and international aircraft operators is scheduled to be completed by the end of 2010. DHS remains committed to completing the implementation of the Secure Flight program in a timely and effective manner.

Section 105(a)(7): Provide for the use of voice stress analysis, biometric, or other technologies to prevent a person who might pose a danger to air safety or security from boarding the aircraft of an air carrier or foreign air carrier in air transportation or intrastate air transportation.

Discussion: TSA regulates airport security access control; however, the airport authorities own/operate the access control systems. Most airports have electronic access control and identification badges, but few have biometrically enabled access control. To facilitate the adoption of biometrics, TSA published the Guidance Package Biometrics for Access Control on September 20, 2005. The Guidance Package establishes basic criteria and standards for the use of biometric technology in airport access control systems. It also includes a list of products and vendors that meet these requirements. In addition, TSA has developed an initial biometric credential interoperability solution, which will be shared with industry for review and comment.

The agency continues to work with the DHS Directorate of Science and Technology to assess Voice Stress Analysis (VSA) software, which uses the physiological characteristics of a human voice pattern to determine its effectiveness in detecting an individual's malevolent or deceptive intent. TSA is assessing the feasibility of conducting VSA at the airport checkpoint.

TSA continues to assess facial recognition technology to determine its effectiveness. The agency is an active participant in the National Science and Technology Council Subcommittee on Biometrics, which is collaborating on biometric research and development across Federal agencies. Facial recognition is an important portion of the Subcommittee's work. Additionally, TSA is coordinating an evaluation of facial recognition and other biometric technologies in an airport operational environment through the National Safe Skies Alliance, which is assessing several facial recognition products in a Checkpoint Surveillance application. As a longer term research project, TSA is planning to conduct and develop a long-range 3D facial recognition and threat detection capability for wide-area surveillance applications.

Status: *Active.* TSA continues to assess the use of voice stress analysis, biometric, or other technologies to determine their effectiveness in airport pre-flight settings.

Section 105(a)(8): Provide for the use of technology that will permit enhanced instant communications and information between airborne passenger aircraft and appropriate individuals or facilities on the ground.

Discussion: TSA is seeking to enhance air-to-ground communications (including air-to-ground, ground-to-air, air-to-air, and intra-cabin) facilitated by the inter-agency public/private sector Air-to-Ground Communications Working Group chaired by TSA. Participation in the Working Group includes, among others, the Department of Transportation (FAA), National Aeronautics and Space Administration (NASA), Department of Justice (Federal Bureau of Investigation), Department of Defense, Department of Homeland Security (TSA, S&T), aviation industry representatives (including domestic airlines and pilots and flight attendants unions), and wireless communications industry representatives.

TSA has developed a Technology Implementation Plan, or Technology Roadmap, and associated public/private partnership business cases for implementation of Air-to-Ground Communications Systems (AGCS) that meet the requirements for critical communications while in flight to assist in intelligence dissemination and awareness.

Implementation of AGCS is vital to provide FAMS with enhanced aviation security situational awareness both on the ground and while in flight. TSA, in close cooperation with NASA, FAA, and other public and private sector stakeholders, is currently engaged in the research, analysis, and technology evaluation, necessary to implement AGCS using a range of commercially owned ground-based and satellite communications links.

The Federal Communication Commission reallocated and auctioned frequency in the 800MHz for commercial air-to-ground communication services. The award of this spectrum to two communication service providers in October 2006 was a critical milestone in developing public-private partnerships to encourage private industry infrastructure investment in narrowband/broadband communication systems and deployment on domestic U.S. commercial passenger aircraft. As a result, TSA is currently working closely with both communication service providers, as well as others using alternative methods, to ensure that their systems will meet TSA air-to-ground communications requirements to the greatest extent possible. The first deployment of these emerging AGCS on a U.S. carrier occurred in December 2007, and TSA participated in the inaugural flight. Fleet-wide pilot implementation on a second U.S. carrier was initiated in early 2008. As a result, several of the testing carriers made the decision to move from a pilot program to airline-wide deployment of the technology on all aircraft types. At this point, TSA intends to use these communication services on a subscription basis to meet FAMS operational needs. This implementation used by the AGCS providers is also available to other local, State, and Federal agencies, as well as airlines, aircrews, and passengers, on a subscription basis.

Additionally, TSA is working with FAA and private companies to develop and test AGCS using existing communications technologies onboard domestic aircraft. First generation Aircraft Communications Addressing and Reporting System (ACARS) is a Very High Frequency (VHF) Data Link (VDL) system that provides data link services involving the transfer of aircraft operations and fleet management data stored in the form of text and character graphic messages. This early standard is often referred to as VDL Mode 1. With performance limitations and demand for greater capabilities, the ARINC Company developed VHF Digital Link Mode 2, or VDLM2, a bit-oriented, air/ground and ground/ground data link technology that delivers information at 31.5 kbps—over 10 times the rate used by legacy ACARS. Several aircraft operators have upgraded portions of their fleet with the newer VDLM2 radio system. The ARINC Company also manages the ACARS ground network, which provides bi-directional (both uplink and downlink) request and reply message capability between aircraft and ground entities.

An AGCS solution capable of using ACARS or VDLM2 was proven in a completed pilot program with Sun Country Airlines and the FAA in April 2008. This pilot system provided the insight and experience that allowed TSA to move forward with an airline and the private sector to engineer and schedule the equipping of two aircraft types. As of late 2008, AGCS is in pilot status on one airline and is in full operational status on four other airlines. As these operational airlines continue to equip their fleets, AGCS will become available on an increasing number of aircraft that TSA covers on a daily basis. TSA continues to work with the airlines that have yet to commit to AGCS technology to discover methods that could allow TSA to gain the necessary communication abilities, while affording the airlines to further analyze the various AGCS possibilities and alternatives that would benefit the airlines and their passengers.

Status: *Active.* TSA is seeking to use commercial narrowband/broadband service for instant communication as it becomes available on all U.S. airlines.

III. CONCLUSION

TSA continues to work to identify enhancements in technology, processes, and procedures to enhance transportation security. This report identifies enhancements that are integrated into the NIPP process. As in prior years, future reporting on the remaining three of the eight items listed under Section 109(a) of ATSA will be included in the Annual Report to Congress on Transportation Security required by title 49 U.S.C. §44938, rather than by separate report. In addition, many of these topics will be regularly discussed with Members of Congress informally and in congressional oversight hearings.

APPENDIX (B) - List of Acronyms

9/11 Act	Implementing Recommendations of the 9/11 Commission Act of 2007
ACARS	Aircraft Communications Addressing and Reporting System
AGCS	Air-to-Ground Communications Systems
ARINC	Aeronautical Radio, Incorporated
AT	Advanced Technology
ATSA	Aviation and Transportation Security Act
BASE	Baseline Assessment for Security Enhancements
BDO	Behavior Detection Officers
BLS	Bottled Liquids Scanners
BWI	Baltimore-Washington Thurgood Marshall International Airport
CBP	Customs and Border Protection
CCSP	Certified Cargo Screening Program
CSR	Corporate Security Review
DHS	Department of Homeland Security
DOT	Department of Transportation
EDCT	Explosives Detection Canine Team
FAA	Federal Aviation Administration (DOT)
FRA	Federal Railroad Administration
FAM	Federal Air Marshal
G8	Group of Eight
GA	General Aviation
GCC	Government Coordinating Council
HAZMAT	Hazardous Materials
HME	Hazardous Material Endorsement
HTUA	High Threat Urban Areas
IAC	Indirect Air Carrier
IBSGP	Intercity Bus Security Grant Program
ICAO	International Civil Aviation Organization
IED	Improvised Explosive Device
IIR	International Industry Representatives
I-STEP	Intermodal Security Training and Exercise Program
LAG	Liquids, Aerosols, and Gels
LASP	Large Aircraft Security Program
LEO	Law Enforcement Officer
MANPADS	Man-Portable Air Defense System
MTSA	Maritime Transportation Security Act of 2002
MVA	MANPADS Vulnerability Assessment Program
NASA	National Aeronautics and Space Administration
NCRCC	National Capital Region Coordination Center
NIPP	National Infrastructure Protection Plan
NLETS	National Law Enforcement Telecommunications
NSTS	National Strategy for Transportation Security
PSGP	Port Security Grant Program

PPID	Positive Pilot Identification
QUAD	Quadrilateral Working Group
R&D	Research and Development
RT	Registered Traveler
RTIP	Registered Traveler Interoperability Pilot
SAI	Security Action Item
S&T	Directorate for Science and Technology (DHS)
SCC	Sector Coordinating Councils
SEACAP	Security Enhancements and Capabilities Augmentation Program
SFBO	Secure Fixed Base Operator
SME	Subject Matter Expert
SSM	Security Sensitive Material
STA	Security Threat Assessments
TDC	Travel Document Checker
TIH	Toxic Inhalation Hazards
TSA	Transportation Security Administration (DHS)
TSAR	Transportation Security Administration Representative
TSGP	Transportation Security Grants Program
TSI	Transportation Security Inspector
TSO	Transportation Security Officer
TSGP	Transportation Security Grant Program
TSS	Transportation Security Specialists
TSSG	Transportation Security Subgroup
TWIC	Transportation Workers Identification Credential
USCG	U.S. Coast Guard (DHS)
VDL	VHF Data Link
VHF	Very High Frequency
VIPR	Visible Intermodal Prevention and Response
VSA	Voice Stress Analysis

APPENDIX (C) -- Congressional Report Recipients

The Honorable Joseph Biden
President of the Senate

The Honorable Nancy Pelosi
Speaker of the House

The Honorable Harry Reid
Senate Majority Leader

The Honorable Mitch McConnell
Senate Minority Leader

The Honorable John Boehner
House Minority Leader

The Honorable John D. Rockefeller
Chairman, Commerce, Science, and Transportation Committee

The Honorable Kay Bailey Hutchison
Ranking Member, Commerce, Science, and Transportation Committee

The Honorable Joseph I. Lieberman
Chairman, Homeland Security and Governmental Affairs Committee

The Honorable Susan M. Collins
Ranking Member, Homeland Security and Governmental Affairs Committee

The Honorable Bennie G. Thompson
Chairman, Homeland Security Committee

The Honorable Peter T. King
Ranking Member, Homeland Security Committee

The Honorable James L. Oberstar
Chairman, Transportation and Infrastructure Committee

The Honorable John L. Mica
Ranking Member, Transportation and Infrastructure Committee

A black and white photograph of the American flag, showing the stars and stripes waving. The flag occupies the top half of the page.

Progress Report on the Transportation Worker Identification Credential Program

In accordance with Section 104 of the Security and Accountability for Every Port Act of 2006, P.L. 109-347
(SAFE Port Act)

August 2009



Homeland
Security

Transportation Security Administration

AUG 18 2009



**Homeland
Security**

Section 104 of the Security and Accountability for Every Port Act of 2006 (SAFE Port Act) (P.L. 109-347) requires the Department of Homeland Security to submit progress reports related to the implementation of TWIC program. Section 104 of the Safe Port Act requires a progress report as follows:

"Not later than 6 months after the date of the enactment of the SAFE Port Act, and every 6 months thereafter until the requirements under this section are fully implemented, the Secretary shall submit a report on the progress being made in implementing such requirements to the appropriate congressional committees"

This document is intended to satisfy this requirement and comprises the fifth 6-month report required by the SAFE Port Act. This letter provides a status update on efforts to implement the GAO recommendation contained in the report and is being provided to the following Members of Congress and the Director of the Office of Management and Budget:

The Honorable Bennie G. Thompson
Chairman, Committee on Homeland Security

The Honorable Peter T. King
Ranking Member, Committee on Homeland Security

The Honorable Joseph I. Lieberman
Chairman, Committee on Homeland Security and Governmental Affairs

The Honorable Susan M. Collins
Ranking Member, Committee on Homeland Security and Governmental Affairs

The Honorable James L. Oberstar
Chairman, Committee on Transportation and Infrastructure

The Honorable John L. Mica
Ranking Member, Committee on Transportation and Infrastructure

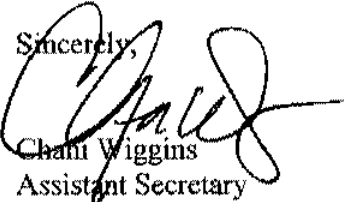
The Honorable John D. Rockefeller IV
Chairman, Committee on Commerce, Science and Transportation

The Honorable Kay Bailey Hutchinson
Ranking Member, Committee on Commerce, Science and Transportation

The Honorable Peter Orszag
Director, Office of Management and Budget

I appreciate your interest in the Department of Homeland Security. If I may be of further assistance, please contact the Office of Legislative Affairs at (202) 447-5890.

Sincerely,



Chanté Wiggins
Assistant Secretary
Office of Legislative Affairs

Foreword

I am pleased to present the following report regarding implementation of the Transportation Worker Identification Credential (TWIC) program. The report has been submitted pursuant to the Security and Accountability for Every Port Act of 2006 (SAFE Port Act) (P.L. 109-347).

The report discusses the progress of the TWIC program. As of April 15, 2009, 1.12 million workers completed the TWIC application process. 1.08 million workers completed the security threat assessment and had their credentials printed, and the remainder were in various stages of the process. 906,956 workers had picked up and activated their cards. At all Captain of the Port Zones, workers must present a TWIC prior to being granted unescorted access to secure areas of facilities or vessels. All mariners that hold a Coast Guard license, certificate of registry, merchant mariner's document or merchant mariner credential must also hold a valid TWIC. The TWIC program's requirements add a layer of security that did not exist just a few months ago, significantly enhancing security at ports across the nation.

Pursuant to statutory requirements, this report is being provided to the Chairmen and Ranking Members of the House Transportation and Infrastructure Committee, the Senate Committee on Commerce, Science, and Transportation, the House Committee on Homeland Security, and the Senate Committee on Homeland Security and Governmental Affairs.

If I may be of further assistance, please do not hesitate to contact me or the TSA Office of Legislative Affairs, at (571) 227-2717.

Sincerely yours,

A handwritten signature in cursive script, reading "Gale D. Rossides".

Gale D. Rossides
Acting Administrator

Executive Summary

The purpose of this report is to transmit the implementation progress of the Transportation Worker Identification Credential (TWIC) program to the House Transportation and Infrastructure Committee, the Senate Committee on Commerce, Science, and Transportation, the House Committee on Homeland Security, and the Senate Committee on Homeland Security and Governmental Affairs. This document is intended to satisfy the reporting requirements of Section 104 of the SAFE Port Act (P.L. 109-347), which requires the Department of Homeland Security to submit progress reports related to the implementation of TWIC program. This document is the fifth 6-month report required by the SAFE Port Act.

The Department of Homeland Security (DHS) manages the TWIC program through the joint participation of the Transportation Security Administration (TSA) and the United States Coast Guard (USCG). The TWIC program provides a tamper-resistant biometric credential to eligible maritime workers requiring unescorted access to secure areas of port facilities and vessels regulated under the Maritime Transportation Security Act of 2002 (MTSA), P.L. 107-295.

TSA completed deployment of the 149 planned enrollment centers in September 2008. TSA continues to operate over 135 enrollment centers located throughout the United States and its territories to serve the estimated 1.2 million maritime workers who will require a TWIC. The Coast Guard began phasing in TWIC enforcement at Captain of the Port (COTP) Zones on a staggered basis beginning October 15, 2008, with national compliance completed April 15, 2009. All ports must now require personnel to present a TWIC to be granted unescorted access to secure areas of facilities and vessels, and all mariners that hold a Coast Guard license, certificate of registry, merchant mariner's document or merchant mariner credential must also hold a valid TWIC. Field reports from the COTP Zones have been generally positive, with the majority of workers having obtained TWICs before the compliance deadline and facilities having enacted appropriate security procedures to support TWIC requirements. As the TWIC program was phased in nationwide, TSA and the Coast Guard closely monitored progress to ensure a smooth transition into compliance.

TSA completed initial capability evaluations of TWIC readers and approved 19 readers for use in the TWIC pilot program; additional readers are expected to undergo testing prior to approval for use in the pilot program. Bench testing of readers continues and is expected to be completed in December 2009. Early operational assessment of readers began in Brownsville, Texas, in April 2009, when the port completed final installation of readers and began operation of TWIC readers at their MTSA-regulated facilities. Three other pilot participants followed Brownsville this summer. The remaining participants are expected to begin operating readers later this year. TSA and the Coast Guard are working towards meeting the SAFE Port Act's requirement to promulgate final regulations for TWIC readers.

The progress on the TWIC program continues to support the Department's goal to protect our nation from dangerous people in the maritime transportation mode.

Table of Contents

I.	Legislative Requirement	1
II.	Background.....	2
III.	Results/Data Report/Expenditure Plan	5
IV.	Analysis/Discussion.....	7
V.	Conclusion/DHS Action Plan.....	10
VI.	Appendix.....	13

I. Legislative Requirement

This document responds to the reporting requirements set forth in the Security and Accountability for Every Port Act of 2006 (SAFE Port Act), P.L. 109-347, Section 104(a), 46 U.S.C. § 70105(l), which requires a report on the progress of the TWIC program and states:

Not later than 6 months after the date of the enactment of the SAFE Port Act, and every 6 months thereafter until the requirements under this section are fully implemented, the Secretary shall submit a report on the progress being made in implementing such requirements to the appropriate congressional committees

II. Background

TWIC is a program of DHS, with joint participation of TSA and the Coast Guard. The TWIC program provides a tamper-resistant biometric credential to all Coast Guard credentialed merchant mariners and to maritime workers requiring unescorted access to secure areas of port facilities and vessels regulated under the Maritime Transportation Security Act of 2002 (MTSA), P.L. 107-295.

The SAFE Port Act required that DHS establish a priority for each port and implement the TWIC program to meet the following schedule milestones:

- Top 10 ports by July 1, 2007
- Next 40 ports by January 1, 2008
- All other ports by January 1, 2009

TSA established priorities for all ports designated for TWIC deployment. On October 16, 2007, TSA began the national deployment of the TWIC program with the enrollment of maritime workers at the Port of Wilmington, Delaware. The top 10 ports were initiated during the first quarter of fiscal year (FY) 2008. Enrollment capabilities were deployed to the next 40 ports in the second quarter of FY 2008. All 149 planned enrollment centers were operational by September 2008. To allow for a full 18-month enrollment period, as established in the TWIC regulation, DHS extended the national compliance date from October 15, 2008, to April 15, 2009.

National deployment of the TWIC program will enhance security of ports by requiring all Coast Guard-credentialed merchant mariners and workers with unescorted access to secure areas of MTSA-regulated vessels and facilities to undergo a security threat assessment and receive a biometric TWIC credential.

The Coast Guard began phasing in enforcement of TWIC regulations at COTP Zones on a staggered basis beginning October 15, 2008, with final national compliance by April 15, 2009. By this deadline:

- all personnel with unescorted access to secure areas of facilities or vessel were required to present a TWIC;
- all mariners that hold a Coast Guard license, certificate of registry, merchant mariner's document or merchant mariner credential were also required to hold a valid TWIC; and
- owners and operators of vessels and outer continental shelf facilities were required to implement TWIC access control procedures.

The Coast Guard announced compliance dates in the Federal Register a minimum of 90 days prior to the start of enforcement.

Port facility and vessel owners and operators will be required to integrate TWIC requirements into their existing access control systems and operations. Based on comments received from the

public following publication of the Notice of Proposed Rulemaking (NPRM)¹ and further analysis, TSA and the Coast Guard concluded that facility and vessel operators would not be required to purchase or install electronic TWIC readers during the first phase of the TWIC program's implementation. An Advanced Notice of Proposed Rulemaking (ANPRM) for TWIC readers was published by the Coast Guard on March 27, 2009 (74 F.R. 13360). Comments received in response to the ANPRM, along with lessons learned from the pilot program, will inform a final rulemaking on the TWIC readers. Until such time, TWICs will be used as visual identity badges for personnel who require access to secure areas of U.S. port facilities and vessels. The objective of the TWIC reader rulemaking is to verify the identity of workers by matching their biometric information with the data stored on the worker's TWIC.

Section 104 of the SAFE Port Act, 46 U.S.C. § 70105(k)(1) requires the Secretary to conduct a TWIC pilot program as follows:

"...to test the business processes, technology, and operational impacts required to deploy transportation security card readers at secure areas of the marine transportation system...at not fewer than 5 distinct geographic locations, to include vessels and facilities in a variety of environmental settings... [and to] commence not later than 180 days after the date of the enactment of the SAFE Port Act."

DHS has entered into formal agreements to conduct pilot tests with the Port of Los Angeles and the Port of Long Beach, the Port Authority of New York and New Jersey; the Port of Brownsville, Texas; the Staten Island Ferry in New York City, the Passenger Vessel Association for a pilot in Annapolis, Maryland; and Magnolia Marine, a towing operator based in Vicksburg, Mississippi. These ports and operations will allow the pilot test to evaluate the impact of using the TWIC for biometric identity verification in the full spectrum of maritime operations and environmental conditions.

TSA has completed three rounds of initial capability testing on TWIC biometric readers and published the list of 19 readers that passed the tests and are approved for use in the pilot program. Functional and environmental specification conformance testing began in the second quarter of FY 2009.

Early operational assessment of readers began in Brownsville, Texas, in April 2009 when the port completed final installation of readers and began operation of TWIC readers at their MTSA-regulated facilities. Three other pilot participants followed Brownsville this summer. The remaining participants are expected to begin operating readers later this year. DHS will use the data gathered during the pilot tests to augment the data previously gathered during TWIC prototype tests in 2005 and 2006. As with the prototype tests, the TWIC pilot tests will involve maritime facilities and port workers and will yield information to support the TWIC reader rulemaking.

TSA and the Coast Guard are working toward meeting the SAFE Port Act's requirement to promulgate final regulations for TWIC readers. The data gathered from the pilot program will be

¹ 71 FR 29396, May 22, 2006.

used to support the Coast Guard's rulemaking activities for TWIC readers. The public will be afforded ample opportunity to comment on the use of biometrics to verify identity at MTSA-regulated vessels and facilities.

III. Results/Data Report/Expenditure Plan

TWIC Enrollment and Compliance Status and Results

TSA completed deployment of the 149 planned enrollment centers in September 2008. TSA continues to operate over 135 enrollment centers located throughout the United States and territories to serve the estimated 1.2 million maritime workers who will require a TWIC.

The Coast Guard began phasing in enforcement of TWIC in COTP Zones on a staggered basis beginning on Oct. 15, 2008, with national compliance completed April 15, 2009, with all ports in compliance and all credentialed mariners required to be in possession of a TWIC. Additionally, the date by which owners and operators of vessels and outer continental shelf facilities were required to implement access control procedures utilizing TWIC was April 15, 2009. The Coast Guard announced compliance dates in the Federal Register a minimum of 90 days prior to the start of each COTP Zone's phased enforcement.

The schedule for Coast Guard compliance and enforcement was completed as follows:

Date	COTP Zone(s)
October 15, 2008	Northern New England Boston Southeastern New England
November 28, 2008	Corpus Christi North Carolina Cape Fear River
December 01, 2008	Buffalo Duluth Detroit Lake Michigan Sault Ste. Marie Long Island Sound Charleston Savannah Jacksonville
December 30, 2008	Baltimore Delaware Bay Lower Mississippi River Mobile Ohio Valley Pittsburgh San Diego
January 13, 2009	Hampton Roads Key West Miami Morgan City New Orleans Upper Mississippi River St. Petersburg

February 12, 2009	Honolulu (except American Samoa) Prince William Sound South East Alaska Western Alaska
February 28, 2009	Portland(OR) Puget Sound San Francisco Bay
March 23, 2009	New York
April 14, 2009	American Samoa Guam Houston/Galveston Los Angeles/Long Beach Port Arthur, TX San Juan

TWIC Reader Pilot Program

The TWIC reader pilot program has been designed to provide data in three areas that will support the TWIC reader rulemaking. These areas are:

- **Bench Testing/Controlled Contactless Reader Testing:** Readers will be tested under controlled conditions to verify that they correctly process biometric information from the credential and can perform that operation in maritime environments.
- **Early Operational Testing:** Facility and vessel operators participating in the TWIC pilots will install readers and begin using them to read TWICs issued to workers. This phase will provide an Early Operational Assessment of reader performance in maritime settings. TSA will gather data to verify the performance of the credentials, readers, and personnel access control systems in the field, and any problems will be identified and corrected before the next, more extensive phase of the pilot.
- **System Test and Evaluation:** Participating facility and vessel operators will verify the identity of all workers needing unescorted access to secure areas of vessels or facilities in accordance with test scenarios that incorporate various options for biometrically verifying identity. This phase will provide data on the impact of the biometric verification process on vessels and facilities, including measuring access wait times, false biometric rejection rates, equipment malfunctions, and implementation costs.

IV. Analysis/Discussion

TWIC Enrollment and Compliance Discussion

As of April 15, 2009, 1.12 million workers completed the TWIC application process. 1.08 million workers completed the security threat assessment and had their credentials printed. 906,956 workers had picked up and activated their cards. The Coast Guard began phasing in TWIC enforcement at COTP Zones on a staggered basis beginning October 15, 2008, with national compliance completed April 15, 2009.

At all COTP Zones, workers must present a TWIC prior to being granted unescorted access to secure areas of facilities or vessels. All mariners that hold a Coast Guard license, certificate of registry, merchant mariner's document or merchant mariner credential must also hold a valid TWIC. The TWIC program's requirements add a layer of security that did not exist just a few months ago, significantly enhancing security at ports across the nation.

Field reports from the COTP Zones have been generally positive, with the majority of workers having obtained TWICs before the compliance deadline and facilities having enacted appropriate security procedures to support TWIC requirements. As the TWIC program was phased in nationwide, TSA and the Coast Guard closely monitored progress to ensure a smooth transition into compliance.

TWIC Reader Pilot Discussion

TSA continues to make progress on the TWIC reader pilot and is expected to complete Bench Testing in December 2009. TSA began the Early Operational Assessment of readers in April 2009. Analysis of each phase of the pilot is provided below.

Bench Testing

Initial Capability Evaluation

TSA issued an initial Broad Agency Announcement (BAA) on June 20, 2008, seeking small and large business sources that can provide Smart Card biometric readers capable of reading TWIC cards. TSA expressed interest in obtaining information on both fixed and handheld portable readers. Card readers must conform to the TWIC Reader Hardware and Card Application Specification and must be available for testing. Subsequent BAAs were issued on August 29, 2008, October 27, 2008, and May 7, 2009 to allow additional manufacturers to submit their readers for testing.

In the BAA, TSA laid out the three-part framework for reader bench testing:

(1) Conduct an initial evaluation of readers to determine their ability to read a TWIC, and from this evaluation, establish a list of readers from which the port, facility, and vessel pilot test participants can choose and acquire the readers best suited for their needs—this is the Initial Capability Evaluation (ICE);

(2) Conduct laboratory tests to assess the conformance of a limited number of readers to the technical and environmental requirements of the TWIC specification—this is the Specification Conformance Test (SCT); and,

(3) Develop a standard test to assess reader compliance with the final TWIC specification for the final TWIC Reader Rule—this is the Final Reader Assessment (FRA).

Respondents to the BAAs issued thus far, whose reader(s) supported the TWIC Privacy Key functionality, have satisfactorily completed the ICE. TSA is conducting the ICE in Charleston, South Carolina. The purpose of the ICE is to demonstrate the ability of a reader to properly recognize, read, and match the biometric on the TWIC to the biometric of the owner of the TWIC using the TWIC Privacy Key capability as provided in the TWIC Card and Reader Specification. The ICE consists of a simple series of tests that can be conducted using production TWICs that will demonstrate the reader's ability to properly read a TWIC in a number of scenarios.

All readers that demonstrate their ability to satisfactorily complete each of the ICE scenarios are included in a published list noting that they have completed the ICE scenarios satisfactorily. Vendors who are Original Equipment Manufacturers (OEMs) or system and equipment integrators were eligible to respond to TSA's BAAs, subject to the limitations described in the Evaluation Criteria section of the announcement. The ICE list will be updated on a regular basis as further rounds of evaluations are conducted. The first ICE list was made available to the public on October 7, 2008, after the first round of testing. The most recent ICE list was published on July 7, 2009 and is available at www.tsa.gov/twic. TSA requires pilot test participants to use the ICE reader list in making reader acquisitions for the pilot test. As of the fourth round of testing, 19 readers passed the ICE test and were approved for use in the pilot.

TSA will keep the May 7, 2009, BAA open throughout most of the pilot to provide an ongoing opportunity for new or previously un-nominated readers to be evaluated using the ICE process. The ICE list will be updated as readers complete a satisfactory evaluation.

Functional and Environmental Specification Conformance Testing

The Government is also conducting reader Specification Conformance Tests (SCTs) in controlled laboratory environments. The results of the SCTs will be published in the final pilot test report. The purpose of these tests is to conduct detailed, precise evaluations to assess the performance of a sampling of readers relative to the TWIC credential and reader specification. The SCTs will enable the Government to assess reader performance in a controlled laboratory environment to provide consistent, controlled measurement and more accurate information than could otherwise be obtained during field tests. Due to the cost and time required to perform the SCTs, the Government will test a limited number of readers (handheld portable and fixed). TSA will make the SCT results available to the public and pilot test participants in the final report.

The purpose of the SCTs is to provide an accurate assessment of the ability of a sampling of readers to meet the TWIC specification, and thus, provide an indication as to the potential for readers to perform well in the maritime environment. The intent of conducting the SCTs is to achieve a comprehensive evaluation; not to establish a list of readers "approved" for use in

accordance with the final TWIC reader rule. The reasons that the Government will not place readers that complete the SCTs on the FRA list are: (1) until the final TWIC reader rule is published, the TWIC specification is considered to be a “working specification”; and, (2) until the final TWIC reader rule is published, the process (if any) for certifying readers for compliance with the rule will not be finalized.

The SCTs consist of two efforts: (1) Functional Specification Conformance Test (F-SCT) -- an evaluation of the technical performance of a reader’s conformance to the card-reading requirements of the specification; and (2) Environmental Specification Conformance Test (E-SCT) -- an evaluation of the ability of a reader to withstand exposure to conditions in the specifications relating to outdoor service (weather conditions, vibration, power fluctuations, among others). Readers for both SCTs were selected from among the readers included on the ICE list. The process and criteria for selecting readers for the functional SCT and environmental SCT were independent of each other. Some readers selected for functional testing were not selected for environmental testing and vice-versa.

Functional and environmental specification conformance testing began in the second quarter of FY 2009.

Early Operational Testing

Pilot operational test planning began with consultations with the ports of Los Angeles and Long Beach in southern California in December 2006. As a result of these discussions, DHS executed cooperative agreements with both Long Beach and Los Angeles. Through the DHS Port Security Grant (PSG) program application process, a number of port, facility, and vessel operators expressed interest in becoming TWIC pilot program participants. Several FY 2007 PSG recipients included facilities and vessels suitable and willing to participate in the TWIC pilot.

One of the goals of the TWIC pilot test is to gather data from a variety of types and sizes of facilities and vessels in various operational and environmental conditions. DHS has entered into formal agreements to conduct pilot tests with the Port of Los Angeles and the Port of Long Beach, the Port Authority of New York and New Jersey; the Port of Brownsville, Texas; the Staten Island Ferry, New York City, the Passenger Vessel Association for a pilot in Annapolis, Maryland; and Magnolia Marine, a towing operator based in Vicksburg, Mississippi. These ports and operations will allow the pilot test to evaluate the impact of using the TWIC for biometric identity verification in the full spectrum of maritime operations and environmental conditions.

Early Operational Assessment began in Brownsville, Texas in April 2009. Three other pilot participants followed Brownsville this summer. The remaining participants are expected to begin operating readers later this year.

System Test and Evaluation

After completing the Early Operational Assessment, System Test and Evaluation (ST&E) will begin. This phase will begin at two sites in September 2009, with others to follow as they complete the EOA phase and complete a readiness evaluation to start the ST&E phase.

V. Conclusion/DHS Action Plan

As of April 15, 2009, 1.12 million workers completed the TWIC application process. 1.08 million workers completed the security threat assessment and had their credentials printed. 906,956 workers had picked up and activated their cards. At all Captain of the Port Zones, workers must present a TWIC prior to being granted unescorted access to secure areas of facilities or vessels

The TWIC reader pilot continues to progress, and data to support the Coast Guard TWIC Reader rulemaking effort will be collected through the pilot. TSA and the Coast Guard are working toward meeting the SAFE Port Act Final Rule requirement to promulgate final regulations for TWIC readers. We are working to execute a pilot program that will allow for the most efficient compilation of information possible, so that it may inform the rulemaking process and provide ample opportunity for the public to comment on the proposals and the pilot data.

The TWIC reader pilot has achieved the following milestones and is tracking to the milestones shown in the table below:

Activity / Milestone	Estimated Completion	Actual Completion	Description
Develop Contactless Card / Reader Specification			
Obtain TWIC Contactless Specification Recommendation from the National Maritime Security Advisory Committee (NMSAC) Note: The smart card reader industry requires the specification integrate TWIC functionality into contactless readers.	28-Feb-07	28-Feb-07	In response to TSA/USCG request, NMSAC recommended a specification enabling the TWIC biometric to be read by contactless readers. The recommended specification included reader performance requirements consistent with operations in the maritime environment.
Publish NMSAC Recommended Specification for Public Comment	Mar-07	16-Mar-07	The comment period was 15 days. Thirty comments were received.
Publish Working Contactless Specification	Aug-07	20-Sept-07	Following a review of comments and technical alignment, TSA published the working specification. Development of contactless readers and the TWIC card application began.
Reader industry delivers first TWIC contactless readers for testing and installation at limited number of test facilities.	FY08 Q3	27-Aug-08	Readers and TWICs with a contactless capability are required prior to beginning pilot testing of contactless performance.
Identify Pilot Test Locations / Sites			
Hold Initial Meetings with Port of Los Angeles / Port of Long Beach	Dec-06	7-Dec-06	DHS/TSA/CG representatives met with POLA/POLB officials to discuss pilot test plans and finalize Cooperative Agreements.

Activity / Milestone	Estimated Completion	Actual Completion	Description
Establish Goals for Gaining Participation of a Variety of Pilot Test Locations / Facilities / Vessels	Mar-07	Mar-07	In conjunction with USCG identified desired mix of facilities / locations / vessels for pilot tests Locations: East Coast, West Coast, Gulf Coast, Great Lakes, Inland Rivers Facilities: container, petro-chemical, bulk cargo, large passenger terminals Vessels: small passenger, ferries, tug and towboats
Hold Initial Meetings with Port of NY / NJ	May-07	1-May-07	Reviewed potential test facilities and their respective advantages / constraints.
Hold Initial Discussions with Port of Brownsville, TX and Passenger Vessel Association (Watermark Cruises of Annapolis, MD)	Jul-07	13-Jul-07	Confirmation of interest in pilot; Port Security Grant status; initiated planning for site visits.
Conduct various site visits to gather detailed baseline and test scenario data.	On-going		
Identify additional primary test participating ports / facilities / vessels	Ongoing		Sites where full data sets of information will be collected will be limited. Additional information will be solicited from those willing to provide it in accordance with test plans. Sites are being added in sufficient numbers to ensure participation goals stated above can be met.
Test Planning			
Establish TWIC Test Planning Working Group (TPWG)	Mar-07	28-Mar-07	DHS established a TPWG which includes system and test engineers and other resources to plan and oversee the pilot test.
Develop TWIC Test and Evaluation Master Plan (TEMP)	Aug-07	14-Dec-07	The TEMP identified the pilot test concept, scope, resources, and test plan requirements. The TEMP is has been reviewed and approved by the TPWG. The TEMP identifies the following critical items: <ul style="list-style-type: none"> ▪ Obtaining / testing readers ▪ Obtaining / testing / issuing contactless TWICs ▪ Obtaining an Independent Test Agent (ITA) to perform test integrator tasks (i.e., plan / oversee tests; collate data; prepare final report). ▪ Design / install tests (the Test Plan) ▪ Coordinate test results with rulemaking requirements
Develop Early Operational Assessment (EOA) Test Plans	FY09 Q3	18-Mar-09	Establishes test plans that will address specific tests to be accomplished during the EOA phase.

Activity / Milestone	Estimated Completion	Actual Completion	Description
Conduct Early Operational Assessment (EOA)	FY10 Q2		EOA is planned to enable rapid gathering of operational reader testing as soon as some readers are available and a larger quantity of workers in the test areas have TWICs with the contactless application.
Conduct Full System Impact Testing (ST&E Phase)	FY10 Q3		Impact testing will require all (or most) workers entering a test facility / vessel to have TWICs. This testing assesses the business and operational impacts of requiring biometric verification of identity in accordance test scenarios which incorporate various options for biometrically verifying identity.
Complete Testing, Prepare Final Test Evaluation and Analysis	FY10 Q4		Interim data will be assessed as the pilot progresses.

VI. Appendix

Congressional Report Recipients

The Honorable James L. Oberstar
Chairman, House Transportation and Infrastructure Committee

The Honorable John L. Mica
Ranking Member, House Transportation and Infrastructure Committee

The Honorable John D. Rockefeller
Chairman, Senate Committee on Commerce, Science, and Transportation

The Honorable Kay Bailey Hutchison
Ranking Member, Senate Committee on Commerce, Science, and Transportation

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

The Honorable Peter T. King
Ranking Member, House Committee on Homeland Security

The Honorable Joseph I. Lieberman
Chairman, Senate Committee on Homeland Security and Governmental Affairs

The Honorable Susan M. Collins
Ranking Member, Senate Committee on Homeland Security and Governmental Affairs



Progress Report on the Transportation Worker Identification Credential Program

In accordance with Section 104 of the Security and
Accountability for Every Port Act of 2006, P.L. 109-347
(SAFE Port Act)

December 2009



**Homeland
Security**

Transportation Security Administration

DEC 03 2009

Foreword

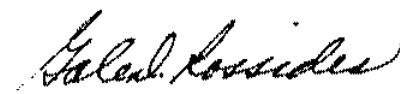
I am pleased to present the following report regarding implementation of the Transportation Worker Identification Credential (TWIC) program. The report has been submitted pursuant to the Security and Accountability for Every Port Act of 2006 (SAFE Port Act) (P.L. 109-347).

The report discusses the progress of the TWIC program. As of October 22, 2009, approximately 1.4 million workers have completed the TWIC application process. Credentials for those applicants determined to be eligible were printed, and approximately 1.3 million workers have activated their cards. At all Captain of the Port Zones, workers must present a TWIC prior to being granted unescorted access to secure areas of facilities or vessels. All mariners that hold a Coast Guard license, certificate of registry, merchant mariner's document or merchant mariner credential must also hold a valid TWIC. The TWIC program's requirements add a layer of security that did not exist previously, significantly enhancing security at ports across the nation.

Pursuant to statutory requirements, this report is being provided to the Chairmen and Ranking Members of the House Transportation and Infrastructure Committee, the Senate Committee on Commerce, Science, and Transportation, the House Committee on Homeland Security, and the Senate Committee on Homeland Security and Governmental Affairs.

If I may be of further assistance, please do not hesitate to contact me or the TSA Office of Legislative Affairs, at (571) 227-2717.

Sincerely yours,

A handwritten signature in cursive script, reading "Gale D. Rossides".

Gale D. Rossides
Acting Administrator

Executive Summary

The purpose of this report is to transmit the implementation progress of the Transportation Worker Identification Credential (TWIC) program to the House Transportation and Infrastructure Committee, the Senate Committee on Commerce, Science, and Transportation, the House Committee on Homeland Security, and the Senate Committee on Homeland Security and Governmental Affairs. This document is intended to satisfy the reporting requirements of Section 104 of the SAFE Port Act (P.L. 109-347), which requires the Department of Homeland Security to submit progress reports related to the implementation of the TWIC program. This document is the sixth 6-month report required by the SAFE Port Act.

The Department of Homeland Security (DHS) manages the TWIC program through the joint participation of the Transportation Security Administration (TSA) and the United States Coast Guard (USCG). The TWIC program provides a tamper-resistant biometric credential to eligible maritime workers requiring unescorted access to secure areas of port facilities and vessels regulated under the Maritime Transportation Security Act of 2002 (MTSA), P.L. 107-295.

TSA completed deployment of the 149 planned enrollment centers in September 2008. TSA continues to operate over 135 enrollment centers located throughout the United States and its territories to serve over 1.3 million maritime workers who require a TWIC. The Coast Guard began phasing in TWIC enforcement at Captain of the Port (COTP) Zones on a staggered basis beginning October 15, 2008, with national compliance completed April 15, 2009. All ports must now require personnel to present a TWIC to be granted unescorted access to secure areas of facilities and vessels, and all mariners that hold a Coast Guard license, certificate of registry, merchant mariner's document or merchant mariner credential must also hold a valid TWIC. Field reports from the COTP Zones have been positive, with the majority of workers having obtained TWICs before the compliance deadline and facilities having enacted appropriate security procedures to support TWIC requirements. In some very limited cases where non-compliance was discovered, action was taken at the COTP level to directly engage with the facility owner/operator to make immediate corrections. In a limited number of cases, enforcement actions (e.g., admin letters of warning or notice of violation) were issued. As the TWIC program was phased in nationwide, TSA and the Coast Guard closely monitored progress to ensure a smooth transition into compliance.

TSA completed initial capability evaluations of TWIC readers and approved 21 readers for use in the TWIC pilot program; additional readers are expected to undergo testing prior to approval for use in the pilot program. Bench testing of readers continues and is expected to be completed in December 2009. The start of testing was delayed to follow a formal source selection process to select readers for testing. Early operational assessment of readers began in Brownsville, Texas, in April 2009 when the port completed final installation of readers and began operation of TWIC readers at their MTSA-regulated facilities. Three other pilot participants followed Brownsville this summer. The remaining participants are expected to begin operating readers later this year. TSA and the Coast Guard are working towards meeting the SAFE Port Act's requirement to promulgate final regulations for TWIC readers.

The progress on the TWIC program continues to support the Department's goal to protect our nation from dangerous people in the maritime transportation mode.

Table of Contents

I.	Legislative Requirement.....	1
II.	Background.....	2
III.	Results/Data Report/Expenditure Plan	5
IV.	Analysis/Discussion.....	7
V.	Conclusion/DHS Action Plan	10
VI.	Appendix	13

I. Legislative Requirement

This document responds to the reporting requirements set forth in the Security and Accountability for Every Port Act of 2006 (SAFE Port Act), P.L. 109-347, Section 104(a), 46 U.S.C. § 70105(l), which requires a report on the progress of the TWIC program and states:

Not later than 6 months after the date of the enactment of the SAFE Port Act, and every 6 months thereafter until the requirements under this section are fully implemented, the Secretary shall submit a report on the progress being made in implementing such requirements to the appropriate congressional committees

II. Background

TWIC is a program of DHS, with joint participation of TSA and the Coast Guard. The TWIC program provides a tamper-resistant biometric credential to all Coast Guard-credentialed merchant mariners and to maritime workers requiring unescorted access to secure areas of port facilities and vessels regulated under the Maritime Transportation Security Act of 2002 (MTSA), P.L. 107-295.

The SAFE Port Act required that DHS establish a priority for each port and implement the TWIC program to meet the following schedule milestones:

- Top 10 ports by July 1, 2007
- Next 40 ports by January 1, 2008
- All other ports by January 1, 2009

TSA established priorities for all ports designated for TWIC deployment. On October 16, 2007, TSA began the national deployment of the TWIC program with the enrollment of maritime workers at the Port of Wilmington, Delaware. The top 10 ports were initiated during the first quarter of fiscal year (FY) 2008. Enrollment capabilities were deployed to the next 40 ports in the second quarter of FY 2008. All 149 planned enrollment centers were operational by September 2008. To allow for a full 18-month enrollment period, as established in the TWIC regulation, DHS extended the national compliance date from October 15, 2008, to April 15, 2009.

National deployment of the TWIC program will enhance security of ports by requiring all Coast Guard-credentialed merchant mariners and workers with unescorted access to secure areas of MTSA-regulated vessels and facilities to undergo a security threat assessment and receive a biometric TWIC credential.

The Coast Guard began phasing in enforcement of TWIC regulations at COTP Zones on a staggered basis beginning October 15, 2008, with final national compliance by April 15, 2009. By this deadline:

- all personnel with unescorted access to secure areas of facilities or vessel were required to present a TWIC;
- all mariners that hold a Coast Guard license, certificate of registry, merchant mariner's document or merchant mariner credential were also required to hold a valid TWIC; and
- owners and operators of vessels and outer continental shelf facilities were required to implement TWIC access control procedures.

The Coast Guard announced compliance dates in the Federal Register a minimum of 90 days prior to the start of enforcement.

Port facility and vessel owners and operators will be required to integrate TWIC requirements into their existing access control systems and operations. Based on comments received from the

public following publication of the Notice of Proposed Rulemaking (NPRM)¹ and further analysis, TSA and the Coast Guard concluded that facility and vessel operators would not be required to purchase or install electronic TWIC readers during the first phase of the TWIC program's implementation. An Advanced Notice of Proposed Rulemaking (ANPRM) for TWIC readers was published by the Coast Guard on March 27, 2009 (74 F.R. 13360). Comments received in response to the ANPRM, along with lessons learned from the pilot program, will inform a final rulemaking on the TWIC readers. Until such time, TWICs will be used as visual identity badges for personnel who require access to secure areas of U.S. port facilities and vessels. The objective of the TWIC reader rulemaking is to verify the identity of workers by matching their biometric information with the data stored on the worker's TWIC.

Section 104 of the SAFE Port Act, 46 U.S.C. § 70105(k)(1) requires the Secretary to conduct a TWIC pilot program as follows:

"...to test the business processes, technology, and operational impacts required to deploy transportation security card readers at secure areas of the marine transportation system...at not fewer than 5 distinct geographic locations, to include vessels and facilities in a variety of environmental settings... [and to] commence not later than 180 days after the date of the enactment of the SAFE Port Act."

DHS has entered into formal agreements to conduct pilot tests with the Port of Los Angeles and the Port of Long Beach, the Port Authority of New York and New Jersey; the Port of Brownsville, Texas; the Staten Island Ferry in New York City, the Passenger Vessel Association for a pilot in Annapolis, Maryland; Magnolia Marine, a towing operator based in Vicksburg, Mississippi; Clipper Navigation, a high-speed ferry operation in Seattle, Washington; and, APM Terminals Virginia, a container facility, in Portsmouth, Virginia. The Staten Island Ferry, Clipper Navigation, and APM Terminals Virginia were added to the pilot since the last six month report to Congress. These ports and operations will allow the pilot test to evaluate the impact of using the TWIC for biometric identity verification in the full spectrum of maritime operations and environmental conditions.

TSA has completed three rounds of initial capability testing on TWIC biometric readers and published the list of 21 readers that passed the tests and are approved for use in the pilot program. Functional and environmental specification conformance testing began in the second quarter of FY 2009.

Early operational assessment of readers began in Brownsville, Texas, in April 2009 when the port completed final installation of readers and began operation of TWIC readers at their Maritime Transportation Security Act of 2002 (MTSA) regulated facilities. Three other pilot participants followed Brownsville this summer. The remaining participants are expected to begin operating readers later this year. DHS will use the data gathered during the pilot tests to augment the data previously gathered during TWIC prototype tests in 2005 and 2006. As with the prototype tests, the TWIC pilot tests will involve maritime facilities and port workers and will yield information to support the TWIC reader rulemaking.

¹ 71 FR 29396, May 22, 2006.

TSA and the Coast Guard are working toward meeting the SAFE Port Act's requirement to promulgate final regulations for TWIC readers. The data gathered from the pilot program will be used to support the Coast Guard's rulemaking activities for TWIC readers. The public will be afforded ample opportunity to comment on the use of biometrics to verify identity at MTSA-regulated vessels and facilities.

III. Results/Data Report/Expenditure Plan

TWIC Enrollment and Compliance Status and Results

TSA completed deployment of the 149 planned enrollment centers in September 2008. TSA continues to operate over 135 enrollment centers located throughout the United States and territories to serve over 1.3 million maritime workers who require a TWIC.

The Coast Guard began phasing in enforcement of TWIC in COTP Zones on a staggered basis beginning on Oct. 15, 2008, with national compliance completed April 15, 2009, with all ports in compliance and all credentialed mariners required to be in possession of a TWIC. Additionally, the date by which owners and operators of vessels and outer continental shelf facilities were required to implement access control procedures utilizing TWIC was April 15, 2009. The Coast Guard announced compliance dates in the Federal Register a minimum of 90 days prior to the start of each COTP Zone's phased enforcement.

The schedule for Coast Guard compliance and enforcement was completed as follows:

Date	COTP Zone(s)
October 15, 2008	Northern New England Boston Southeastern New England
November 28, 2008	Corpus Christi North Carolina Cape Fear River
December 01, 2008	Buffalo Duluth Detroit Lake Michigan Sault Ste. Marie Long Island Sound Charleston Savannah Jacksonville
December 30, 2008	Baltimore Delaware Bay Lower Mississippi River Mobile Ohio Valley Pittsburgh San Diego
January 13, 2009	Hampton Roads Key West Miami Morgan City New Orleans Upper Mississippi River St. Petersburg

February 12, 2009	Honolulu (except American Samoa) Prince William Sound South East Alaska Western Alaska
February 28, 2009	Portland(OR) Puget Sound San Francisco Bay
March 23, 2009	New York
April 14, 2009	American Samoa Guam Houston/Galveston Los Angeles/Long Beach Port Arthur, TX San Juan

TWIC Reader Pilot Program

The TWIC reader pilot program has been designed to provide data in three areas that will support the TWIC reader rulemaking. These areas are:

- Bench Testing/Controlled Contactless Reader Testing: Readers will be tested under controlled conditions to verify that they correctly process biometric information from the credential and can perform that operation in maritime environments.
- Early Operational Testing: Facility and vessel operators participating in the TWIC pilots will install readers and begin using them to read TWICs issued to workers. This phase will provide an Early Operational Assessment of reader performance in maritime settings. TSA will gather data to verify the performance of the credentials, readers, and personnel access control systems in the field, and any problems will be identified and corrected before the next, more extensive phase of the pilot.
- System Test and Evaluation: Participating facility and vessel operators will verify the identity of all workers needing unescorted access to secure areas of vessels or facilities in accordance with test scenarios that incorporate various options for biometrically verifying identity. This phase will provide data on the impact of the biometric verification process on vessels and facilities, including measuring access wait times, false biometric rejection rates, equipment malfunctions, and implementation costs.

IV. Analysis/Discussion

TWIC Enrollment and Compliance Discussion

As of October 22, 2009, approximately 1.4 million workers completed the TWIC application process. Of those that were determined to be eligible for a TWIC, approximately 1.3 million have picked up and activated their cards. The Coast Guard began phasing in TWIC enforcement at COTP Zones on a staggered basis beginning October 15, 2008, with national compliance completed April 15, 2009.

At all COTP Zones, workers must present a TWIC prior to being granted unescorted access to secure areas of facilities or vessels. All mariners that hold a Coast Guard license, certificate of registry, merchant mariner's document or merchant mariner credential must also hold a valid TWIC. The TWIC program's requirements add a layer of security that did not exist just a few months ago, significantly enhancing security at ports across the nation.

Field reports from the COTP Zones have been generally positive, with the majority of workers having obtained TWICs before the compliance deadline and facilities having enacted appropriate security procedures to support TWIC requirements. As the TWIC program was phased in nationwide, TSA and the Coast Guard closely monitored progress to ensure a smooth transition into compliance.

TWIC Reader Pilot Discussion

TSA continues to make progress on the TWIC reader pilot and is expected to complete bench testing in December 2009. The start of bench testing was delayed to conduct a formal process in accordance with contracting rules to select readers to be tested. This was done to ensure that all qualified reader vendors would have an equal opportunity to have their readers selected for testing. TSA began the Early Operational Assessment of readers in April 2009. Analysis of each phase of the pilot is provided below.

Bench Testing

Initial Capability Evaluation

TSA issued an initial Broad Agency Announcement (BAA) on June 20, 2008, seeking small and large business sources that can provide Smart Card biometric readers capable of reading TWIC cards. TSA expressed interest in obtaining information on both fixed and handheld portable readers. Card readers must conform to the TWIC Reader Hardware and Card Application Specification and must be available for testing. Subsequent BAAs were issued on August 29, 2008, October 27, 2008, and May 7, 2009 to allow additional manufacturers to submit their readers for testing.

In the BAA, TSA laid out the three-part framework for reader bench testing:

- (1) Conduct an initial evaluation of readers to determine their ability to read a TWIC, and from this evaluation, establish a list of readers from which the port, facility, and vessel pilot test

participants can choose and acquire the readers best suited for their needs—this is the Initial Capability Evaluation (ICE);

(2) Conduct laboratory tests to assess the conformance of a limited number of readers to the technical and environmental requirements of the TWIC specification—this is the Specification Conformance Test (SCT); and,

(3) Develop a standard test to assess reader compliance with the final TWIC specification for the final TWIC Reader Rule—this is the Final Reader Assessment (FRA).

Respondents to the BAAs issued thus far, whose reader(s) supported the TWIC Privacy Key functionality, have satisfactorily completed the ICE. TSA is conducting the ICE in Charleston, South Carolina. The purpose of the ICE is to demonstrate the ability of a reader to properly recognize, read, and match the biometric on the TWIC to the biometric of the owner of the TWIC using the TWIC Privacy Key capability as provided in the TWIC Card and Reader Specification. The ICE consists of a simple series of tests that can be conducted using production TWICs that will demonstrate the reader's ability to properly read a TWIC in a number of scenarios.

All readers that demonstrate their ability to satisfactorily complete each of the ICE scenarios are included in a published list noting that they have completed the ICE scenarios satisfactorily. Vendors who are Original Equipment Manufacturers (OEMs) or system and equipment integrators were eligible to respond to TSA's BAAs, subject to the limitations described in the Evaluation Criteria section of the announcement. The ICE list will be updated on a regular basis as further rounds of evaluations are conducted. The first ICE list was made available to the public on October 7, 2008, after the first round of testing. The most recent ICE list was published on July 7, 2009 and is available at www.tsa.gov/twic. TSA requires pilot test participants to use the ICE reader list in making reader acquisitions for the pilot test. As of the fourth round of testing, 21 readers passed the ICE test and were approved for use in the pilot.

TSA will keep the May 7, 2009 BAA open throughout most of the pilot to provide an ongoing opportunity for new or previously un-nominated readers to be evaluated using the ICE process. The ICE list will be updated as readers complete a satisfactory evaluation.

Functional and Environmental Specification Conformance Testing

The Government is also conducting reader Specification Conformance Tests (SCTs) in controlled laboratory environments. The results of the SCTs will be published in the final pilot test report. The estimated completion of the pilot test report is late 2010. The purpose of these tests is to conduct detailed, precise evaluations to assess the performance of a sampling of readers relative to the TWIC credential and reader specification. The SCTs will enable the Government to assess reader performance in a controlled laboratory environment to provide consistent, controlled measurement and more accurate information than could otherwise be obtained during field tests. Due to the cost and time required to perform the SCTs, the Government will test a limited number of readers (handheld portable and fixed). TSA will make the SCT results available to the public and pilot test participants in the final report.

The purpose of the SCTs is to provide an accurate assessment of the ability of a sampling of readers to meet the TWIC specification, and thus, provide an indication as to the potential for readers to perform well in the maritime environment. The intent of conducting the SCTs is to achieve a comprehensive evaluation; not to establish a list of readers “approved” for use in accordance with the final TWIC reader rule. The reasons that the Government will not place readers that complete the SCTs on the FRA list are: (1) until the final TWIC reader rule is published, the TWIC specification is considered to be a “working specification”; and, (2) until the final TWIC reader rule is published, the process (if any) for certifying readers for compliance with the rule will not be finalized.

The SCTs consist of two efforts: (1) Functional Specification Conformance Test (F-SCT) -- an evaluation of the technical performance of a reader’s conformance to the card-reading requirements of the specification; and (2) Environmental Specification Conformance Test (E-SCT) -- an evaluation of the ability of a reader to withstand exposure to conditions in the specifications relating to outdoor service (weather conditions, vibration, power fluctuations, among others). Readers for both SCTs were selected from among the readers included on the ICE list. The process and criteria for selecting readers for the functional SCT and environmental SCT were independent of each other. Some readers selected for functional testing were not selected for environmental testing and vice-versa.

Functional and environmental specification conformance testing began in the second quarter of FY 2009. TSA completed functional tests on four readers; tests of at least two additional readers will be scheduled for October. All actual environmental tests were completed in October. Five readers were tested, and the environmental test report is expected by the end of October.

Early Operational Testing

Pilot operational test planning began with consultations with the ports of Los Angeles and Long Beach in southern California in December 2006. As a result of these discussions, DHS executed cooperative agreements with both Long Beach and Los Angeles. Through the DHS Port Security Grant (PSG) program application process, a number of port, facility, and vessel operators expressed interest in becoming TWIC pilot program participants. Several FY 2007 PSG recipients included facilities and vessels suitable and willing to participate in the TWIC pilot.

One of the goals of the TWIC pilot test is to gather data from a variety of types and sizes of facilities and vessels in various operational and environmental conditions. DHS has entered into formal agreements to conduct pilot tests with the Port of Los Angeles and the Port of Long Beach, the Port Authority of New York and New Jersey; the Port of Brownsville, Texas; the Staten Island Ferry, New York City, the Passenger Vessel Association for a pilot in Annapolis, Maryland; Magnolia Marine, a towing operator based in Vicksburg, Mississippi; Clipper Navigation, a high-speed ferry operation in Seattle, Washington; and, APM Terminals Virginia, a container facility, in Portsmouth, Virginia. The Staten Island Ferry, Clipper Navigation, and APM Terminals Virginia were added to the pilot since the last six month report to Congress. These ports and operations will allow the pilot test to evaluate the impact of using the TWIC for biometric identity verification in the full spectrum of maritime operations and environmental conditions.

The Early Operational Assessment (EOA) test phase began in Brownsville, Texas in April 2009. EOA testing also began at three small vessel operations and the Staten Island Ferry in the spring and summer. EOA testing at the ports of New York/New Jersey, Los Angeles, and Long Beach plus one terminal in Portsmouth, Virginia is expected to begin the remainder of this year and into 2010. The ports of New York/New Jersey, Los Angeles, and Long Beach incurred delays in completing site plans, obtaining authorizations to expend pilot funds from the Federal Emergency Management Agency (FEMA), and awarding reader installation contracts. These difficulties resulted in delays in starting and completing the EOA and System Test and Evaluation phases of the test. The new estimated completion dates for these phases is shown in the table at the end of this report.

System Test and Evaluation

Each individual test site will begin System Test and Evaluation (ST&E) after completing the Early Operational Assessment. The ST&E phase will begin at two sites this fall with others to follow as they complete the EOA phase.

V. Conclusion/DHS Action Plan

As of October 22, 2009, approximately 1.4 million workers completed the TWIC application process. Of those that were determined to be eligible for a TWIC, approximately 1.3 million have picked up and activated their cards. At all Captain of the Port Zones, workers must present a TWIC prior to being granted unescorted access to secure areas of facilities or vessels

The TWIC reader pilot continues to progress, and data to support the Coast Guard TWIC Reader rulemaking effort will be collected through the pilot. TSA and the Coast Guard are working toward meeting the SAFE Port Act Final Rule requirement to promulgate final regulations for TWIC readers. We are working to execute a pilot program that will allow for the most efficient compilation of information possible, so that it may inform the rulemaking process and provide ample opportunity for the public to comment on the proposals and the pilot data.

The TWIC reader pilot has achieved the following milestones and is tracking to the milestones shown in the table below:

Activity / Milestone	Estimated Completion	Actual Completion	Description
Develop Contactless Card / Reader Specification			
Obtain TWIC Contactless Specification Recommendation from the National Maritime Security Advisory Committee (NMSAC) Note: The smart card reader industry requires the specification integrate TWIC functionality into contactless readers.	28-Feb-07	28-Feb-07	In response to TSA/USCG request, NMSAC recommended a specification enabling the TWIC biometric to be read by contactless readers. The recommended specification included reader performance requirements consistent with operations in the maritime environment.
Publish NMSAC Recommended Specification for Public Comment	Mar-07	16-Mar-07	The comment period was 15 days. Thirty comments were received.
Publish Working Contactless Specification	Aug-07	20-Sept-07	Following a review of comments and technical alignment, TSA published the working specification. Development of contactless readers and the TWIC card application began.
Reader industry delivers first TWIC contactless readers for testing and installation at limited number of test facilities.	FY08 Q3	27-Aug-08	Readers and TWICs with a contactless capability are required prior to beginning pilot testing of contactless performance.
Identify Pilot Test Locations / Sites			
Hold Initial Meetings with Port of Los Angeles / Port of Long Beach	Dec-06	7-Dec-06	DHS/TSA/CG representatives met with POLA/POLB officials to discuss pilot test plans and finalize Cooperative Agreements.

Activity / Milestone	Estimated Completion	Actual Completion	Description
Establish Goals for Gaining Participation of a Variety of Pilot Test Locations / Facilities / Vessels	Mar-07	Mar-07	In conjunction with USCG identified desired mix of facilities / locations / vessels for pilot tests Locations: East Coast, West Coast, Gulf Coast, Great Lakes, Inland Rivers Facilities: container, petro-chemical, bulk cargo, large passenger terminals Vessels: small passenger, ferries, tug and towboats
Hold Initial Meetings with Port of NY / NJ	May-07	1-May-07	Reviewed potential test facilities and their respective advantages / constraints.
Hold Initial Discussions with Port of Brownsville, TX and Passenger Vessel Association (Watermark Cruises of Annapolis, MD)	Jul-07	13-Jul-07	Confirmation of interest in pilot; Port Security Grant status; initiated planning for site visits.
Conduct various site visits to gather detailed baseline and test scenario data.	On-going		
Identify additional primary test participating ports / facilities / vessels	Ongoing		Sites where full data sets of information will be collected will be limited. Additional information will be solicited from those willing to provide it in accordance with test plans. Sites are being added in sufficient numbers to ensure participation goals stated above can be met.
Test Planning			
Establish TWIC Test Planning Working Group (TPWG)	Mar-07	28-Mar-07	DHS established a TPWG which includes system and test engineers and other resources to plan and oversee the pilot test.
Develop TWIC Test and Evaluation Master Plan (TEMP)	Aug-07	14-Dec-07	The TEMP identified the pilot test concept, scope, resources, and test plan requirements. The TEMP was reviewed and approved by the TPWG. The TEMP identifies the following critical items: <ul style="list-style-type: none"> Obtaining / testing readers Obtaining / testing / issuing contactless TWICs Obtaining an Independent Test Agent (ITA) to perform test integrator tasks (i.e., plan / oversee tests; collate data; prepare final report). Design / install tests (the Test Plan) Coordinate test results with rulemaking requirements
Develop Early Operational Assessment (EOA) Test Plans	FY09 Q3	18-Mar-09	Established test plans that addressed specific tests to be accomplished during the EOA phase.

Activity / Milestone	Estimated Completion	Actual Completion	Description
Conduct Early Operational Assessment (EOA)	FY10 Q2		EOA is planned to enable rapid gathering of operational reader testing as soon as some readers are available and a larger quantity of workers in the test areas have TWICs with the contactless application.
Conduct Full System Impact Testing (ST&E Phase)	FY10 Q3		Impact testing will require all (or most) workers entering a test facility / vessel to have TWICs. This testing assesses the business and operational impacts of requiring biometric verification of identity in accordance test scenarios which incorporate various options for biometrically verifying identity.
Complete Testing, Prepare Final Test Evaluation and Analysis	FY10 Q4		Interim data will be assessed as the pilot progresses.
Deliver Final TWIC Pilot Test Report to Congress	FY11-Q1		Deliver report required by the SAFE Port Act.

VI. Appendix

Congressional Report Recipients

The Honorable James L. Oberstar
Chairman, House Transportation and Infrastructure Committee

The Honorable John L. Mica
Ranking Member, House Transportation and Infrastructure Committee

The Honorable John D. Rockefeller
Chairman, Senate Committee on Commerce, Science, and Transportation

The Honorable Kay Bailey Hutchison
Ranking Member, Senate Committee on Commerce, Science, and Transportation

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

The Honorable Peter T. King
Ranking Member, House Committee on Homeland Security

The Honorable Joseph I. Lieberman
Chairman, Senate Committee on Homeland Security and Governmental Affairs

The Honorable Susan M. Collins
Ranking Member, Senate Committee on Homeland Security and Governmental Affairs

FOR OFFICIAL USE ONLY



Explosives Detection Systems

Fiscal Year 2009 Report to Congress

1st and 2nd Quarter Update

August 14, 2009



Homeland
Security

Transportation Security Administration

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Message from the Acting Administrator of the Transportation Security Administration

August 14, 2009

I am pleased to present the following report, "Explosives Detection Systems," which has been prepared by the Transportation Security Administration.

This document has been compiled in response to requirements in the Fiscal Year 2009 Department of Homeland Security Appropriations Act (P.L. 110-329) and the accompanying Explanatory Statement and Senate Report 110-396. It provides an expenditure plan update for the procurement and installation of emerging technologies and advanced threat detection systems for airport passenger checkpoints.

Pursuant to Congressional requirements, this report is being provided to the following Members of Congress:

The Honorable David E. Price
Chairman, House Appropriations Subcommittee on Homeland Security

The Honorable Harold Rogers
Ranking Member, House Appropriations Subcommittee on Homeland Security

The Honorable Robert C. Byrd
Chairman, Senate Appropriations Subcommittee on Homeland Security

The Honorable George V. Voinovich
Ranking Member, Senate Appropriations Subcommittee on Homeland Security

If I may be of further assistance, please do not hesitate to contact me at (571) 227-2845 or the Department's Acting Chief Financial Officer, Peggy Sherry, at (202) 447-5751.

Sincerely yours,



Gale D. Rossides
Acting Administrator

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Executive Summary

The Fiscal Year (FY) 2009 Department of Homeland Security Appropriations Act (P.L. 110-329) and the accompanying Explanatory Statement and Senate Report 110-396 require the Department to provide a quarterly expenditure plan update for Checkpoint Support and include information on specific technologies for purchase, project timelines, a schedule for obligation and a table detailing actual versus anticipated unobligated balances at the close of the fiscal year.

The EDS installation and purchase funding is implemented through the Electronic Baggage Screening program (EBSP). The EBSP oversees the screening of all baggage checked in airports nationwide. EBSP tests, procures, deploys, integrates and provides life cycle support for approximately 7,700 pieces of security equipment that screen checked baggage at approximately 450 of the Nation's airports.

EBSP allocates resources to airport baggage screening facility modification projects, purchase and installation of explosives detection system technology and technology initiatives aimed at improving operational effectiveness and efficiencies, as well as the programmatic resources required to ensure effective execution of the program.

This report reflects one deviation from the original plan through the 1st and 2nd quarters to the FY 2009 Spend Plan. The change is explained in the Appendix D, Obligation Data.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY



Explosives Detection Systems 1st and 2nd Quarter Update

Table of Contents

I.	Legislative Requirement	1
II.	Electronic Baggage Screening Program	2
	A. Background	2
	B. Expenditure Plan	6
III.	Appendices	11
	Appendix A: Abbreviations/Acronyms	12
	Appendix B: Airport Codes	13
	Appendix C: Deployment by Project	15
	Appendix D: EBSP Summary Spend Plan	18
	Appendix E: EBSP Obligation Data	25
	Appendix F: EBSP Milestones	33
	Appendix G: Actual vs. Anticipated Unobligated Balance	43

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

I. Legislative Requirement

This report is provided in compliance with requirements in the Fiscal Year (FY) 2009 Department of Homeland Security Appropriations Act (P.L. 110-329) and the accompanying Explanatory Statement and Senate Report 110-396, which include the following language.

P.L. 110-329 includes the following provisions:

EXPLOSIVES DETECTION SYSTEMS

As discussed in the Senate report, TSA shall provide quarterly updates on EDS and checkpoint expenditures, on an airport-by-airport basis. These updates shall include information on the specific technologies for purchase, project timelines, a schedule for obligation, and a table detailing actual versus anticipated unobligated balances at the close of the fiscal year, with an explanation of any deviation from the original plan.

The Explanatory Statement offers the following guidance:

As discussed in the Senate report, TSA shall provide quarterly updates on EDS and checkpoint expenditures, on an airport-by-airport basis. These updates shall include information on the specific technologies for purchase, project timelines, a schedule for obligation, and a table detailing actual versus anticipated unobligated balances at the close of the fiscal year, with an explanation of any deviation from the original plan.

In addition, Senate Report 110-396 includes the following:

EXPENDITURE PLANS FOR EDS/CHECKPOINT TECHNOLOGIES

Additionally, the Committee includes a new requirement for the expenditure plans to be updated quarterly and to include the following new information: specific technologies planned for purchase; project timelines; a schedule for obligation; and a table detailing actual unobligated balances versus anticipated unobligated balances at the close of the fiscal year. The quarterly updates shall also include an explanation for any deviation from the original plan.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

II. Electronic Baggage Screening Program

A. Background

Mission

The Electronic Baggage Screening Program's (EBSP's) mission is central to the Transportation Security Administration (TSA) mission area covering "the range of TSA activities that minimize the risk of injury or death of people or damage or loss of property due to hostile acts of terrorism that may be directed against the National Airspace System." Preventing catastrophic loss and air piracy involves verifying that checked baggage carries no prohibited items or items that have been identified as threat objects for the particular transportation mode. The screening process targets the checked baggage of all people boarding aircraft through the use of screening security systems.

EBSP tests, acquires, deploys, integrates and maintains the technology that screens passenger checked baggage to deter, detect, mitigate and prevent transportation of explosives or other prohibited items on commercial aircraft while ensuring freedom of movement for people and commerce.

Purpose

EBSP was initiated by the White House Commission on Aviation Safety and Security at the Federal Aviation Administration in 1997. In response to the events of September 11, 2001, a Congressional mandate transferred the EBSP to DHS. Furthermore, public laws were enacted to accelerate and dramatically increase the scope of the EBSP. The Aviation and Transportation Security Act (ATSA), P.L. 107-71, stated that all checked baggage must be screened at all the nation's airports with an explosives detection system or a suitable alternative as soon as possible, but not later than December 31, 2002. The Homeland Security Act of 2002 (HSA), P.L. 107-296, later granted DHS a waiver until December 31, 2003, to screen all checked baggage at all airports, a condition that was met.

EBSP is currently in a "mixed" acquisition life cycle, focusing predominately on the purchase, deployment and sustainment phases of the acquisition process. The primary technologies acquired and deployed under the EBSP are Explosives Detection System (EDS) equipment and Explosives Trace Detector (ETD) devices. The following three technology configurations comply with the mandates of ATSA and the HSA:

1. ETD-based systems – Transportation Security Officers (TSOs) use ETD machines as a primary method to screen bags.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

2. Stand-alone EDS systems – TSOs also use EDS machines as a primary method to screen bags. Alarmed bags are resolved by ETDs.
3. Inline EDS systems – TSOs use EDS machines as a primary method to screen bags. Alarmed bags are resolved by ETDs.

Using EDS technology (both inline and standalone) is preferred over using ETDs as a primary screening method due to:

(b)(3);49 U.S.C. § 114(r)

(detailed performance capabilities are classified). Improving security supports TSA and DHS goals of Prevent and Protect.

2. Increased Efficiency – EDS machines have a higher throughput than ETD units used in primary screening, decreasing lobby congestion and passenger wait time. Higher baggage throughput supports TSA's goal of "ensuring freedom of movement for people and commerce."
3. Decreased Labor Costs – EDS configurations at larger airports require fewer TSOs to operate than ETDs used in primary screening configurations. Increased automation reduces human error and personnel costs. EDS machines also have reduced operating costs over the life of the equipment and require less lifting of baggage, thus reducing the number of on-the-job injuries.

These technologies have been in production since 1997, and production is expected to continue indefinitely with enhancements both to engineering and detection capabilities. EBSP currently manages seven technology vendors and sixteen technology models, and provides life-cycle procurement, deployment, integration and maintenance of more than 7,700 units of security equipment at approximately 450 federalized U.S. airports. To date, EBSP has supplied 68 airports with full optimal systems and enabled some screening areas with optimal systems at 52 additional airports.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

The following chart shows the enacted/appropriated funding since inception of the EDS/ETD Install and Purchase Program, Project and Activity (PPA).

Program Project and Activity	FY 2002 Enacted	FY 2002 Supplemental	FY 2003 Enacted	FY 2003 Supplemental	FY 2004 Enacted	FY 2005 Enacted	FY 2006 Enacted	FY 2007 Enacted	FY 2007 Supplemental	FY 2008 Enacted	FY 2009 Enacted
EDS/ETD Purchase	\$859,800,000		\$174,500,000		\$150,000,000	\$180,000,000	\$175,000,000	\$141,400,000		\$294,000,000	\$294,000,000
EDS/ETD Installation		\$738,000,000	\$265,000,000	\$235,000,000	\$250,000,000	\$295,000,000	\$295,000,000	\$388,000,000		\$250,000,000	\$250,000,000
Total, EDS/ETD Purchase and Installation	\$859,800,000	\$738,000,000	\$439,500,000	\$235,000,000	\$400,000,000	\$475,000,000	\$470,000,000	\$529,400,000	\$285,000,000	\$544,000,000	\$544,000,000

*Includes \$250M Aviation Security Capital Fund (ASCF) fee beginning in FY 2007

Goal

The EBSPP supports Goal Two of the DHS Strategic Plan, FYs 2008–2013, “Protect Our Nation from Dangerous Goods.”

EBSPP fulfills the Congressional mandate for 100-percent screening of aviation checked baggage by electronic or other approved means (found in ATSA, Section 110).

The mandate to screen 100 percent of checked baggage has been achieved, and on-going efforts to operate, maintain and improve screening systems remains critical. In particular, it is imperative that the Program continue to research, evaluate and deploy refinements to EDS and EDT technology and associated systems that allow for improvements in:

1. Throughput (checked bags per hour);
2. The false-alarm rate;
3. System availability; and
4. Total cost of ownership for baggage screening (cost per checked bag).

In addition, there exists the need to re-locate equipment from airport lobby areas to baggage room areas.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid “need-to-know” without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Program Progress to Date (Relative to EDS/ETD deployment and facility modifications)

EDS/ETD Purchase/Installation Historical Funding

	<u>Purchase</u>	<u>Install</u>	<u>Units/EDS</u>	<u>Units/ETDs</u>	<u>Agreements</u>	<u>% Agreements awarded*</u>	<u>% Install awarded**</u>
FY 2004							
Enacted	149,700	249,000	136	24	19	100	100
FY 2005							
Enacted	180,000	295,000	134	248	3	100	100
FY 2006							
Enacted	175,000	295,000	216	552	17	100	100
FY 2007							
Enacted***	141,400	388,000	133	529	7	100	100
FY 2007, Supplemental							
Enacted	285,000		48	0	6	100	100
FY 2008							
Enacted***	544,000		114	3	10	100	95
FY 2009							
Enacted***	544,000		129	0	11		

*Agreements awarded: percent of planned project OTA/LOIs awarded either in the year funding was appropriated or the following year with carryover funding

**Installs awarded: percent of planned airport projects completed with EDS/ETD purchased and installed equipment either in the year funding was appropriated or the following year with the available carryover funding. The FY08 planned purchase and installation projects will be completed in FY09 with available carryover funding.

***Includes \$250M Aviation Security Capital Fund fees

Per Congressional direction, EBSP allocates funding among a wide variety of airports ranging from non-hub to large. When EBSP nears the achievement of its optimal solution, funding allocation will begin to shift from primarily purchase and install costs to operations and management and recapitalization costs as the need for new installations

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

B. Expenditure Plan

Summary of FY 2009 EBSP Expenditure Plan

Section	\$ in Millions
Program Operations and Management	74.9
LOI	200.0
Other Transactional Agreement (OTA) - New Facility Modification Agreement Projects	82.5
EDS Purchase and Install	146.6
Technology/Engineering Initiatives	40.0
Total	544.0

The FY 2009 Spend Plan totals \$544 million in FY 2009 enacted level:

- Total FY 2009 Purchase Funds equal \$107.7 million of enacted FY 2009 funds
- Total FY 2009 Install Funds equal \$436.3 million, which includes \$186.3 million of enacted FY 2009 funds and \$250 million Airport Security Capital Funds

Total project costs represent incurred costs: original equipment procurement, manufacturer installation, integration, multiplexing, warehousing, shipping, testing and facility modifications.

Facility modification amounts are based upon FY 2009 Application information and TSA cost validation process. The amount is subject to change due to updated cost submittals and negotiations with the airport.

TSA has identified a total of three LOIs, eight airports for facility modifications and 42 airports for Purchase and Installations.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Supporting Data

Estimated Number of Optimal Systems

Category	Total Number of TSA Airports	Entire Airport with Optimal Systems	Some Screening Areas with Optimal Systems	Total Number of Airports with at least one Optimal System	Percentage of Airports with at least one Optimal System	Optimal Systems Inline Projects Funded FY 2009*
X	27	5	17	22	81%	2
I	55	15	17	32	58%	3
II	73	27	15	42	58%	6
III	122	21	3	24	20%	10
Total	277	68	52	120	43%	21

*FY 2009 and ARRA funds include reduced size EDS purchase for ETD-only airports.

Expenditure Plan

Expenditure Plan: Appropriations, Obligations, and Expenditures

PROGRAM SPENDING PLAN: EBSP

APPROPRIATIONS IN \$ MILLIONS

Net Appropriated Funds ¹	544.000
Project Outlays End-of-Q2 FY09	14.177
Funds Obligated, Not Outlaid End-of-Q2 FY FY09	26.935
Unobligated Balance End-of-Q2 FY09	502.888

UNOBLIGATED BALANCES BY FY as of 31 MAR 2009²

FY09	Total
502.888	502.888

PLANNED OBLIGATIONS IN \$ MILLIONS AS OF 31 MAR 2009

	Q1FY09	Q2FY09 ⁴	Q3FY09	Q4FY09	Q1FY10	Q2FY10	Q3FY10	Q4FY10
Plan ³	18.727	70.074	247.875	207.323	-	-	-	-
Plan Cumulative	18.727	88.801	336.677	544.000	544.000	544.000	544.000	544.000
% Allotment	10.30%	38.44%	0.00%	0.00%	n/a	n/a	n/a	n/a
Actual	1.929	26.935						

PLANNED OUTLAYS IN \$ MILLIONS AS OF 31 MAR 2009

	Q1FY09	Q2FY09	Q3FY09	Q4FY09	Q1FY10	Q2FY10	Q3FY10	Q4FY10
Plan ⁵	18.727	52.556	203.425	134.911	134.381			
Plan Cumulative	18.727	71.283	274.708	409.619	544.000	544.000	544.000	544.000
% Allotment	10.30%	23.30%	0.00%	0.00%	n/a	n/a	n/a	n/a
Actual	1.929	12.248						

1. Total of all FY09 appropriations, actual and planned obligations, and actual and planned expenditures

2. Obtained from Status of Funds, Mar.31 2009

3. Q1FY09 and Q2FY09 reflects actuals, Q3FY09 - Q4 FY09 includes Planned FY09 O&M, LOI, EDS Purchase & Install, OTA, and Engineering

4. Q2FY09 figure includes the Procurement of Reduced Size Machines per the FY09 Spend Plan. Q4FY09 figure includes Procurement of Medium Sized EDS equipment. Excludes LAX OTA; Administrative Modification in place to assign LAX OTA to correct activity code.

5. Q1FY09 Planned outlays includes Q1 and Q2FY09 actuals. Q3FY09 and onwards assumes 75% of planned obligations will have outlays in the same period, with the remaining 25% outlays occurring in the subsequent period.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Program Initiatives

Description of Initiative I – Program Operations and Management

- Description: The Program Operations and Management initiative is broken down into five sections.
 1. Operations and Compliance/Interim Solutions
 - Moves, Adds, and Changes \$7.4 million
 - Equipment Warehousing \$3.5 million
 2. Program Support
 - Program, Resource, and Data Management Services \$16.0 million
 - Testing Services \$3.0 million
 - Audits, Travel, Training, and Certification \$1.2 million
 3. Engineering Support
 - Integration and Installation Management \$13.5 million
 - Engineering Technical and Design Support \$10.5 million
 4. TSA Systems Integration Facility (TSIF) Support \$4.8 million
 5. Personnel Compensation & Benefits (PC&B) \$15.0 million
- Projected Obligations and Expenditures: **\$74.9 million**

Description of Initiative II – LOI

- Previously committed multi-year agreements for facility modifications
- Projected Obligations and Expenditures: **\$200.0 million**

Description of Initiative III – EDS will be purchased and installed for:

- FY 2009
 - Equipment for new terminals to permit TSA to screen bags on opening day to ensure that the airports do not rely on other screening solutions
 - Equipment necessary to maintain 100-percent screening compliance at existing installations
 - Equipment to fulfill existing TSA facility modification agreements (e.g., EDS machines for LOI or OTA airports) for optimal in-line screening solutions that remove lobby congestion and decrease security concerns
 - Equipment to airports that have not received facility modifications funding, but are proceeding with optimal system projects via their own financing and are most cost effective
- Projected Obligations and Expenditures: **\$146.6 million**
- Activities and Milestones: Installs based on airport schedules

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Description of Initiative IV - New Facility Modification Agreements

- Description: OTAs will be used to fund facility modifications to construct a Checked Baggage Inspection System (CBIS) at eight airports.
- 3. See Appendix G for Obligation data
 - See Appendix H for Milestones
 - Projected Obligations and Expenditures: **\$82.5 million**

Description of Initiative V – Technology/Engineering Initiatives

- COTR/Engineering Initiatives will address:
 - Design and configuration changes/modifications (includes reconfiguration requirements and Engineering Change Proposals [ECP])
 - Change in government guidance/objectives to improve efficiencies and equipment performance, such as employing equipment upgrades across the entire fleet of EDS (example: performance upgrade all CT-80 to CT-80DR), and implementing local networking at sites with multiple CT-80/CT-80DR systems to improve data collection efficiencies.
 - Problems with repairs associated with equipment redeployment and out-of warranty/non-operational issues
 - Lack of commonality among checked baggage screening solutions
 - Limitations on deployment of screening solutions based on existing site conditions
 - Variances in technology capabilities that limit TSA flexibility in providing optimal screening solutions
 - Projected Obligations and Expenditures: Total Engineering Initiatives: **\$25.0 million**
- Advanced Surveillance Program (ASP) will address:
 - Remote visibility into the baggage resolution and screening areas in case of
 - Emergency to aid in threat identification and response
 - A means to create an overall situational awareness to support oversight control for
 - Loss prevention, remote supervision, training, staffing, performance evaluation and
 - Legal or investigative needs with recordation
 - An additional layer of security into the locations that TSA screens checked baggage
 - Reduction of threat risks being introduced into checked baggage
 - Projected Obligations and Expenditures: Total ASP Initiatives: **\$5.0 million**
- Security Technology Integrated Program (STIP) will address:
 - Equipment in-service upgrades and automated data retrieval on equipment and screener performance to increase equipment availability, reliability and effectiveness; improve performance management; and reduce overall operating and support costs.
 - Equipment replacement, reconfiguration, and deployment strategies to increase throughput, systems capacity, and effectiveness.
 - Projected Obligations and Expenditures: Total STIP Initiatives: **\$8.0 million**

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

- Operational Integration (OI) will address:
 - System integration and equipment purchases required for operational test and evaluation activities.
 - Projected Obligations and Expenditures: Total OI Initiatives: **\$2.0 million**
- Projected Obligations and Expenditures: Total Technology/Engineering Initiatives: **\$40 million**

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

III. Appendices

- A. Abbreviations/Acronyms
- B. Airport Codes
- C. Deployment by Project
- D. EBSP Summary Spend Plan
- E. EBSP Obligation Data
- F. EBSP Milestones
- G. Actual vs. Anticipated Unobligated Balance

FOR OFFICIAL USE ONLY

Appendix A: Abbreviations/Acronyms

ASP	Advanced Surveillance Program
CBIS	Checked Baggage Inspection System
COTR	Contracting Officer's Technical Representative
EDS	Explosives Detection Systems
LOI	Letter of Intent
OI	Operations Integration
OTA	Other Transaction Agreement
PC&B	Personnel Compensation and Benefits
STIP	Security Technology Integrated Program
TSA	Transportation Security Administration
TSIF	TSA Systems Integration Facility

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix B: Airport Codes

Airport Code	Airport Name	Airport Location
ACK	Nantucket Memorial	Nantucket, MA
AMA	Rick Husband Amarillo International	Amarillo, TX
ASE	Aspen-Pitkin County/Sardy Field	Aspen, CO
CHA	Lovell Field	Chattanooga, TN
CHS	Charleston AFB/International	Charleston, SC
CMI	University of Illinois – Willard	Savoy, IL
CVG	Cincinnati/Northern Kentucky International	Covington, KY
EGE	Eagle County Regional	Eagle, CO
EWB	Newark Liberty International	Newark, NJ
FAT	Fresno Yosemite International	Fresno, CA
GPI	Glacier Park International	Kalispell, MT
GUC	Gunnison-Crested Butte Regional	Gunnison, CO
HDN	Yampa Valley	Hayden, CO
HLN	Helena Regional	Helena, MT
IAH	George Bush Intercontinental/Houston	Houston, TX
ICT	Wichita Mid-Continent	Wichita, KS
ITO	Hilo International	Hilo, HI
JFK	John F. Kennedy	New York, NY
LGA	La Guardia	New York, NY
LSE	La Crosse Municipal	La Crosse, WI
MCO	Orlando International	Orlando, FL
MFR	Rogue Valley International – Medford	Medford, OR
MIA	Miami International	Miami, FL
MKK	Molokai Airport	Kaunakakai, HI
MSP	Minneapolis – St Paul International/Wold-Chamberlain	Minneapolis, MN
OGG	Kahului	Maui, HI
ORD	Chicago O’Hare International	Chicago, IL
PFN	Panama City-Bay County International	Panama City, FL
PHL	Philadelphia International	Philadelphia, PA
PHX	Phoenix Sky Harbor International Airport	Phoenix, AZ
PIT	Pittsburgh International	Pittsburgh, PA

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid “need-to-know” without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Airport Code	Airport Name	Airport Location
PNS	Pensacola Regional	Pensacola, FL
RDM	Roberts Field	Redmond, OR
RDU	Raleigh-Durham International	Raleigh, NC
RNO	Reno/Tahoe International	Reno, NV
ROC	Greater Rochester International	Rochester, NY
SAN	San Diego International	San Diego, CA
SAT	San Antonio International	San Antonio, TX
SFO	San Francisco International	San Francisco, CA
SBA	Santa Barbara Municipal	Santa Barbara, CA
SJC	Norman Y. Mineta San Jose International	San Jose, CA
SMX	Santa Maria Public Airport	Santa Maria, CA
SNA	John Wayne Airport-Orange County	Orange County, CA
SUN	Friedman Memorial	Hailey, ID
TLH	Tallahassee Regional	Tallahassee, FL
TRI	Tri-Cities Regional TN/VA	Bristol/Johnson/Kingsport, TN
TUS	Tucson International	Tucson, AZ
UTA	Tunica Municipal	Tunica, MS

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix C: Obligation by Project

Project	Spend Plan	Project Timelines				Project Cost		Obligation Schedule		Obligation Balances			Expenditures
		Ant. Start Date	Actual Start Date	Ant. End Date	Actual End Date	Initial Dollar Amt.	Revised Dollar Amt.	Planned Obligation	Actual Obligation	Obligated	Unobligated Balance	Anticipated Unobligated	
JFK	LOI	Sep-08	Sep-08	Sep-13	-	\$78.00	-	May-09	-	\$0.00	\$78.00	\$0.00	
EWB	LOI	Sep-08	Sep-08	Sep-13	-	\$60.00	-	May-09	-	\$0.00	\$60.00	\$0.00	
LGA	LOI	Sep-08	Sep-08	Sep-13	-	\$62.00	-	May-09	-	\$0.00	\$62.00	\$0.00	
ORD	OTA	Aug-09	-	Feb-10	-	\$19.80	-	May-09	-	\$0.00	\$19.80	\$0.00	
ICT	OTA	Dec-09	-	Jan-11	-	\$8.25	-	Sep-09	-	\$0.00	\$8.25	\$0.00	
SAT	OTA	Nov-09	-	Dec-11	-	\$24.00	-	Sep-09	-	\$0.00	\$24.00	\$0.00	
FAT	OTA	Sep-09	-	Jan-11	-	\$3.75	-	Jun-09	-	\$0.00	\$3.75	\$0.00	
MSP	OTA	Nov-09	-	Apr-13	-	\$8.00	-	Sep-09	-	\$0.00	\$8.00	\$0.00	
TRI	OTA	Jan-09	-	Sep-09	-	\$3.25	-	Sep-09	-	\$0.00	\$3.25	\$0.00	
AMA	OTA	Mar-09	-	Jan-11	-	\$8.25	-	Sep-09	-	\$0.00	\$8.25	\$0.00	
PFN	OTA	Jul-09	-	Mar-10	-	\$7.25	-	Sep-09	-	\$0.00	\$7.25	\$0.00	
Medium Throughput EDS	Purchase	Mar-09	-	Sep-09	-	\$84.74	-	Mar-09	-	\$0.00	\$84.74	\$0.00	
Reduced Size EDS	Purchase	Jan-09	Mar-09	Sep-09		\$23.00	-	Jan-09	Mar-09	\$19.52	\$3.48	\$0.00	
EWB	Install	Oct-09	-	May-09	-	\$1.21	-	Oct-09	-	\$0.00	\$1.21	\$0.00	
ORD	Install	Dec-09	-	Jun-09	-	\$1.55	-	Dec-09	-	\$0.00	\$1.55	\$0.00	
CVG	Install	Aug-09	Mar-09	Mar-09	-	\$2.16	-	Aug-09	Mar-09	\$0.67	\$1.49	\$0.00	
MCO	Install	Aug-09	Apr-09	Mar-09	-	\$2.65	-	Aug-09	Mar-09	\$0.72	\$1.93	\$0.00	
MIA	Install	Sep-09	Apr-09	Apr-09	-	\$2.63	-	Sep-09	Mar-09	\$0.75	\$1.88	\$0.00	
IAH	Install	Dec-09	-	May-09	-	\$1.55	-	Dec-09	-	\$0.00	\$1.55	\$0.00	
ACK	Install	Feb-09	-	Feb-09	-	\$0.12	-	Feb-09	-	\$0.00	\$0.12	\$0.00	
SAT	Install	Oct-09	-	Aug-09	-	\$2.42	-	Oct-09	-	\$0.00	\$2.42	\$0.00	
PFN	Install	Dec-09	-	Jun-09	-	\$0.92	-	Dec-09	-	\$0.00	\$0.92	\$0.00	
SJC	Install	Jul-09 & Jan-10	-	Mar-10 & Sep-10	-	\$2.92	-	Jul-09	-	\$0.00	\$2.92	\$0.00	
AMA	Install	May-09	-	May-09	-	\$0.82	-	May-09	-	\$0.00	\$0.82	\$0.00	
MFR	Install	Feb-09	Feb-09	Feb-09	-	\$1.04	-	May-09	Feb-09	\$0.76	\$0.28	\$0.00	
TLH	Install	Nov-09	-	Jun-09	-	\$1.03	-	Nov-09	-	\$0.00	\$1.03	\$0.00	
OGG	Install	Aug-09	-	Mar-10		\$1.10	-	Aug-09	-	\$0.00	\$1.10	\$0.00	

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Project	Spend Plan	Project Timelines				Project Cost		Obligation Schedule		Obligation Balances			Expenditures
		Ant. Start Date	Actual Start Date	Ant. End Date	Actual End Date	Initial Dollar Amt.	Revised Dollar Amt.	Planned Obligation	Actual Obligation	Obligated	Unobligated Balance	Anticipated Unobligated	
PHX	Install	Aug-09	-	Mar-09	-	\$0.45	-	Aug-09	-	\$0.00	\$0.45	\$0.00	
PNS	Install	Jan-09	-	Mar-09	-	\$0.12	-	Jul-09	-	\$0.00	\$0.12	\$0.00	
RDU	Install	Mar-09	-	Oct-09	-	\$0.00	-	Mar-09	-		\$0	\$0.00	
RNO	Install	Jul-09	-	Jul-09	-	\$0.90	-	Aug-09	-	\$0.00	\$0.90	\$0.00	
ROC	Install	May-09	-	May-09	-	\$0.00	-	May-09	-	\$0.00		\$0.00	
SAN	Install	Aug-09	Mar-09	Mar-09	-	\$0.24	-	Aug-09	Feb-09	\$0.18	\$0.06	\$0.00	
SFO	Install	Jan-09	-	Apr-09	-	\$1.43	-	Jan-09	-	\$0.00	\$1.43	\$0.00	
SNA	Install	Nov-09	-	Jun-09	-	\$2.11	-	Nov-09	-	\$0.00	\$2.11	\$0.00	
LSE	Install	May-09	-	May-09	-	\$0.08	-	May-09	-	\$0.00	\$0.08	\$0.00	
PIT	Install	Aug-09	-	Aug-09	-	\$0.08	-	Aug-09	-	\$0.00	\$0.08	\$0.00	
SMX	Install	Jun-09	-	Jun-09	-	\$0.08	-	Jun-09	-	\$0.00	\$0.08	\$0.00	
ITO	Install	Jun-09	-	Jun-09	-	\$0.08	-	Jun-09	-	\$0.00	\$0.08	\$0.00	
GPI	Install	Jun-09	-	Jun-09	-	\$0.08	-	Jun-09	-	\$0.00	\$0.08	\$0.00	
MKK	Install	Jun-09	-	Jun-09	-	\$0.08	-	Jun-09	-	\$0.00	\$0.08	\$0.00	
HLN	Install	Jun-09	-	Jun-09	-	\$0.08	-	Jun-09	-	\$0.00	\$0.08	\$0.00	
CHA	Install	Mar-09	-	Mar-09	-	\$0.08	-	Mar-09	-	\$0.00	\$0.08	\$0.00	
CHS	Install	Feb-09	-	Feb-09	-	\$0.26	-	Feb-09	-	\$0.00	\$0.26	\$0.00	
CMI	Install	Apr-09	-	Apr-09	-	\$0.08	-	Apr-09	-	\$0.00	\$0.08	\$0.00	
SUN	Install	Apr-09	-	Apr-09	-	\$0.08	-	Apr-09	-	\$0.00	\$0.08	\$0.00	
GUC	Install	May-09	-	May-09	-	\$0.08	-	May-09	-	\$0.00	\$0.08	\$0.00	
SAN-RS	Install	Apr-09	-	Apr-09	-	\$0.60	-	Apr-09	-	\$0.00	\$0.60	\$0.00	
PHL-RS	Install	May-09	-	May-09	-	\$0.89	-	May-09	-	\$0.00	\$0.89	\$0.00	
HDN	Install	May-09	-	May-09	-	\$1.24	-	May-09	-	\$0.00	\$1.24	\$0.00	
EGE	Install	Jun-09	-	Jun-09	-	\$0.72	-	Jun-09	-	\$0.00	\$0.72	\$0.00	
ASE**	Install	Replaced with SBA	-	Replaced with SBA	-	\$0.00	-	Project cancelled and replaced with SBA	-			\$0.00	
SBA**	Install	Jul-09	-	Jul-09	-	\$0.72	-	Jul-09	-	\$0.00	\$0.72	\$0.00	
TUS	Install	Mar-09	-	Mar-09	-	\$0.33	-	Mar-09	-	\$0.00	\$0.33	\$0.00	
UTA	Install	Jun-09	-	Jun-09	-	\$0.08	-	Jun-09	-	\$0.00	\$0.08	\$0.00	
RDM	Install	Feb-09	-	Feb-09	-	\$0.72	-	Feb-09	-	\$0.00	\$0.72	\$0.00	
Recap	Install		-		-	\$5.00	-		-	\$0.00	\$5.00	\$0.00	

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know", without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Project	Spend Plan	Project Timelines				Project Cost		Obligation Schedule		Obligation Balances			Expenditures
		Ant. Start Date	Actual Start Date	Ant. End Date	Actual End Date	Initial Dollar Amt.	Revised Dollar Amt.	Planned Obligation	Actual Obligation	Obligated	Unobligated Balance	Anticipated Unobligated	
COTR/ Engineering Initiatives	T&E		-		-	\$25.00		Ongoing thru Sept	n/a	\$2.07	\$22.93	\$3.80	
STIP	T&E		-		-	\$8.00	-	Ongoing thru Sept	n/a	\$1.03	\$6.97	\$0.00	
ASP	T&E		-		-	\$5.00	-	Ongoing thru Sept	n/a	\$0.00	\$5.00	\$0.00	
OI	T&E		-		-	\$2.00	-	Ongoing thru Sept	n/a	\$0.00	\$2.00	\$0.00	
Ops & Compliance, Program Support, Engineering Support, TSIF Support, & PC&B	P.O & M		-		-	\$74.90	-	Ongoing thru Sept	n/a	\$15.40	\$59.50	\$0.02	

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix D: EBSP Summary Spend Plan

Summary

Section	\$ in Millions
Program Operations and Management	\$74.9
LOI	\$200.0
OTA - New Facility Modification Agreement Projects	\$146.6
EDS Purchase and Install	\$82.5
Technology/Engineering Initiatives	\$40.0
Total	\$544.0

Program Operations and Management

Project Description	Total TSA FY 2009 Project Cost
Operations and Compliance/Interim Solutions	
- Moves, Adds and Changes	\$7.4
- Equipment Warehousing	\$3.5
Program Support	
- Program, Resource and Data Management Services	\$16.0
- Testing Services	\$3.0
- Audits, Travel, Training and Certification	\$1.2
Engineering Support	
- Integration and Installation Management	\$13.5
- Engineering Technical and Design Support	\$10.5
TSA Systems Integration Facility (TSIF) Support	\$4.8
Personnel Compensation & Benefits (PC&B)	\$15.0
Total	\$74.9

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

LOI Projects

Airport	Scope of Work	TSA Cost Share	Total TSA FY 2009 Project Cost
JFK	LOI funding for the airport to construct a CBIS for Terminals 2, 3, 4, & 7.	90%	\$78.0
EWR	LOI funding for the airport to construct a CBIS for Terminals A, B, & C.	90%	\$60.0
LGA	LOI funding for the airport to construct a CBIS for Terminals USAir & CTB	90%	\$62.0
Total LOI Projects			\$200.0

OTA - New Facility Modification Agreement Projects

Airport	Scope of Work	TSA Cost Share*	Total TSA FY 2009 Project Cost
ORD	OTA funding for the airport to construct a CBIS for Terminal 1-B South	90%	\$19.8
ICT	OTA funding for the airport to construct a CBIS for Terminal Main	95%	\$8.25
SAT	OTA funding for the airport to construct a CBIS for Terminal 1/B	90%	\$24.0
FAT	OTA funding for the airport to construct a CBIS for Terminal Main	95%	\$3.75
MSP	OTA funding for the airport to construct a CBIS for the Lindbergh Terminal	90%	\$8.0
TRI	OTA funding for the airport to construct a CBIS for Terminal Main	95%	\$3.25
AMA	OTA funding for the airport to construct a CBIS for Terminal Main	95%	\$8.25
PFN	OTA funding for the airport to construct a CBIS for New Terminal	95%	\$7.25
Total OTA			\$82.5

*TSA's cost share in this table is 90% for a project at a medium or large hub airport and 95% for a project at a small and non-hub airport.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

FY 2009 EDS Purchase & Install Projects

Airport	Scope of Work	Purchase	Deployment	TSA Cost Share*	Total TSA FY 2009 Project Cost
EWR	Purchase, install, integrate, network and test (3) Medium Speed EDS.	\$3.24	\$1.24	100%	\$4.48
ORD	Purchase, install, integrate, network and test (4) Medium Speed EDS for Terminal 1. B-South.	\$4.32	\$1.55	100%	\$5.87
CVG	Purchase, install, integrate, network and test (5) Medium Speed EDS for Terminal 3.	\$5.40	\$2.16	100%	\$7.56
MCO	Purchase, install, integrate, network and test (7) Medium Speed EDS for Terminal Central East.	\$7.56	\$2.65	100%	\$10.21
MIA	Purchase, install, integrate, network and test (8) Medium Speed EDS for Terminal East/Cruise Matrix.	\$8.64	\$2.63	100%	\$11.27
IAH	Purchase, install, integrate, network and test (4) Medium Speed EDS for Terminal D.	\$4.32	\$1.55	100%	\$5.87
ACK	Purchase, install and test (1) Reduced Size EDS for Terminal Main.	\$0.42	\$0.12	100%	\$0.54
SAT	Purchase, install, integrate, network and test (7) Medium Speed EDS for Terminal 1/B	\$7.56	\$2.42	100%	\$9.98
PFN	Purchase, install, integrate, network and test (2) Medium Speed EDS for Terminal New	\$2.16	\$0.92	100%	\$3.08
SJC	Purchase, install, integrate, network and test (8) Medium Speed EDS for Terminal A/B.	\$9.72	\$2.92	100%	\$12.64
AMA	Purchase, install, integrate, network and test (2) Reduced Size EDS for Terminal Main.	\$0.84	\$0.82	100%	\$1.66

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Airport	Scope of Work	Purchase	Deployment	TSA Cost Share*	Total TSA FY 2009 Project Cost
MFR	Purchase, install, integrate, network and test (2) Reduced Size EDS for Terminal Main	\$0.84	\$1.04	100%	\$1.88
TLH	Purchase, install, integrate, network and test (2) Medium Speed EDS for Terminal Main	\$2.16	\$1.03	100%	\$3.19
OGG	Install, integrate, network and test (3) Medium Speed EDS for Terminal Main.	\$-	\$1.10	100%	\$1.10
PHX	Purchase, install, integrate, network and test (1) Medium Speed EDS for Terminal 4	\$1.08	\$0.45	100%	\$1.53
PNS	Purchase, install, integrate, network and test (1) Medium Speed EDS for Terminal Main.	\$0.42	\$0.12	100%	\$0.54
RDU	Purchase of (2) Medium Speed EDS for Terminal C West.	\$2.16	\$-	100%	\$2.16
RNO	Install, integrate, network, and test (3) Reduced Size EDS for Terminal Main.	\$-	\$0.90	100%	\$0.90
ROC	Purchase of (6) Reduced Size EDS for Terminal Main.	\$2.53	\$-	100%	\$2.53
SAN	Purchase, install, integrate, network, and test (1) Medium Speed EDS for Terminal 2 East.	\$1.08	\$0.24	100%	\$1.32
SFO	Purchase, install, integrate, network and test (4) Medium Speed EDS for Terminal C.	\$4.32	\$1.43	100%	\$5.75
SNA	Purchase, install, integrate, network and test (4) Medium Speed EDS for Terminal C.	\$4.32	\$2.11	100%	\$6.43
LSE	Purchase, install and test (1) Reduced Size EDS for Terminal Main.	\$0.42	\$0.08	100%	\$0.50

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Airport	Scope of Work	Purchase	Deployment	TSA Cost Share*	Total TSA FY 2009 Project Cost
PIT	Purchase, install and test (1) Reduced Size EDS for Terminal Main.	\$0.42	\$0.08	100%	\$0.50
SMX	Purchase, install and test (1) Reduced Size EDS for Terminal Main.	\$0.42	\$0.08	100%	\$0.50
ITO	Purchase, install and test (1) Reduced Size EDS for Terminal Main.	\$0.42	\$0.08	100%	\$0.50
GPI	Purchase, install and test (1) Reduced Size EDS for Terminal Main.	\$0.42	\$0.08	100%	\$0.50
MKK	Purchase, install and test (1) Reduced Size EDS for Terminal Main.	\$0.42	\$0.08	100%	\$0.50
HLN	Purchase, install and test (1) Reduced Size EDS for Terminal Main.	\$0.42	\$0.08	100%	\$0.50
CHA	Purchase, install and test (1) Reduced Size EDS for Terminal Main.	\$0.42	\$0.08	100%	\$0.50
CHS	Purchase, install and test (3) Reduced Size EDS for Terminal Main.	\$1.26	\$0.26	100%	\$1.52
CMI	Purchase, install and test (1) Reduced Size EDS for Terminal Main.	\$0.42	\$0.08	100%	\$0.50
SUN	Purchase, install and test (1) Reduced Size EDS for Terminal Main.	\$0.42	\$0.08	100%	\$0.50
GUC	Purchase, install and test (1) Reduced Size EDS for Terminal Main.	\$0.42	\$0.08	100%	\$0.50
SAN-RS	Purchase, install, integrate, network and test (5) Reduced Size EDS for Terminal I.	\$2.10	\$0.60	100%	\$2.70

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Airport	Scope of Work	Purchase	Deployment	TSA Cost Share*	Total TSA FY 2009 Project Cost
PHL-RS	Purchase, install, integrate, network, and test (3) Reduced Size EDS for Terminal B/C.	\$1.26	\$0.89	100%	\$2.16
HDN	Install, integrate, network and test (3) Reduced Size EDS for Terminal Main.	\$-	\$1.24	100%	\$1.24
EGE	Purchase, install and test (1) Reduced Size EDS for Terminal Main.	\$0.84	\$0.72	100%	\$1.56
ASE**	Purchase, install, integrate, network and test (2) Reduced Size EDS for Terminal Main.				
SBA**	Purchase, install, integrate, network and test (2) Reduced Size EDS for Terminal Main.	\$0.84	\$0.72	100%	\$1.56
TUS	Purchase, install, integrate, network and test (2) Reduced Size EDS for Terminal Main.	\$1.68	\$0.33	100%	\$2.02
UTA	Purchase, install, integrate, network and test (2) Reduced Size EDS for Terminal Main.	\$0.42	\$0.08	100%	\$0.5
RDM	Purchase, install, integrate, network and test (2) Reduced Size EDS for Terminal Main.	\$0.84	\$0.72	100%	\$1.56
Recapitalization		\$20.75	\$5.0	100%	\$25.75
Total Purchase and Install		\$107.7	\$38.0		\$146.6

*TSA funds 100% of the Purchase and Install costs associated with each project

** ASE was canceled and replaced with SBA

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Technology/Engineering Initiatives

Project Description	Total TSA FY 2009 Project Cost
COTR/Engineering Initiatives	\$25.0
Security Technology Integrated Program (STIP)	\$8.0
Advanced Surveillance Program (ASP)	\$5.0
Operations Integration (OI)	\$2.0
Total	\$40.0

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix E: EBSP Obligation Data

Obligation Schedule

Obligation dates and selected airports are subject to change based on airport schedules and contract negotiations.

Airport	Scope of Work	Project Cost \$ in Millions	Planned Obligation Date
Program Operations & Management			
N/A	Ops & Compliance, Program Support, Engineering Support, TSIF Support and PC&B	\$74.9	Ongoing thru Sept
LOI Projects			
JFK	LOI Funding for the airport to construct a CBIS for Terminals 2, 3, 4 & 7.	\$78.0	May 2009
EWR	LOI funding for the airport to construct a CBIS for Terminals A, B & C.	\$60.0	May 2009
LGA	LOI funding for the airport to construct a CBIS for Terminals USAir & CTB	\$62.0	May 2009
EDS Install & Purchase Projects			
EWR	Purchase, install, integrate, network and test (3) Medium Speed EDS.	\$4.48	P-Jun I-Oct
ORD	Purchase, install, integrate, network and test (4) Medium Speed EDS for Terminal 1B-South.	\$5.87	P-Jun I-Dec
CVG	Purchase, install, integrate, network and test (5) Medium Speed EDS for Terminal 3.	\$7.56	P-Jun I-Aug
MCO	Purchase, install, integrate, network and test (7) Medium Speed EDS for Terminal Central East.	\$10.21	P-Jun I-Aug
MIA	Purchase, install, integrate, network and test (8) Medium Speed EDS for Terminal East/Cruise Matrix.	\$11.27	P-Jun I-Sep
IAH	Purchase, install, integrate, network and test (4) Medium Speed EDS for Terminal D.	\$5.87	P-Jun I-Dec
ACK	Purchase, install, and test (1) Reduced Size EDS for Terminal Main.	\$0.54	P-Jan I-Feb
SAT	Purchase, install, integrate, network and test (7) Medium Speed EDS for Terminal 1/B.	\$9.98	P-Jun I-Oct
PFN	Purchase, install, integrate, network and test (2) Medium Speed EDS for Terminal New.	\$3.08	P-Jun I-Dec

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Airport	Scope of Work	Project Cost \$ in Millions	Planned Obligation Date
EDS Install & Purchase Projects (Cont.)			
SJC	Purchase, install, integrate, network and test (8) Medium Speed EDS for Terminal A/B.	\$12.64	P-Jun I-Jul (4) Dec (4)
AMA	Purchase, install, integrate, network and test (2) Reduced Size EDS for Terminal Main.	\$1.66	P-Mar I-May
MFR	Purchase, install, integrate, network and test (2) Reduced Size EDS for Terminal Main.	\$1.88	P-Jan I-May
TLH	Purchase, install, integrate, network and test (2) Medium Speed EDS for Terminal Main.	\$3.19	P-Jun I-Nov
OGG	Install, integrate, network and test (3) Medium Speed EDS for Terminal Main.	\$1.10	P-warehouse* I-Aug
PHX	Purchase, install, integrate, network and test (1) Medium Speed EDS for Terminal 4.	\$1.53	P-Jan I-Aug
PNS	Purchase, install, integrate, network and test (1) Medium Speed EDS for Terminal Main.	\$0.54	P-Jan I-Jul
RDU	Purchase of (2) Medium Speed EDS for Terminal C West.	\$2.16	P-Sep I-Mar 2010
RNO	Install, integrate, network and test (3) Reduced Size EDS for Terminal Main.	\$0.90	P-relocation* I-Aug
ROC	Purchase of (6) Reduced Size EDS for Terminal Main.	\$2.53	P-Mar I-May *
SAN	Purchase, install, integrate, network and test (1) Medium Speed EDS for Terminal 2 East.	\$1.32	P-Jan I-Aug
SFO	Purchase, install, integrate, network and test (4) Medium Speed EDS for Terminal 2.	\$5.75	P-Jun I-Jan 10
SNA	Purchase, install, integrate, network and test (4) Medium Speed EDS for Terminal C.	\$6.43	P-Jun I-Nov
LSE	Purchase, install and test (1) Reduced Size EDS for Terminal Main.	\$0.50	P-Mar I-May
PIT	Purchase, install and test (1) Reduced Size EDS for Terminal Main.	\$0.50	P-Mar I-Aug
SMX	Purchase, install and test (1) Reduced Size EDS for Terminal Main.	\$0.50	P-Mar I-Jun
ITO	Purchase, install and test (1) Reduced Size EDS for Terminal Main.	\$0.50	P-Mar I-Jun

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Airport	Scope of Work	Project Cost \$ in Millions	Planned Obligation Date
EDS Install & Purchase Projects (Cont)			
GPI	Purchase, install and test (1) Reduced Size EDS for Terminal Main.	\$0.50	P-Mar I-Jun
MKK	Purchase, install and test (1) Reduced Size EDS for Terminal Main.	\$0.50	P-Mar I-Jun
HLN	Purchase, install and test (1) Reduced Size EDS for Terminal Main.	\$0.50	P-Mar I-Jun
CHA	Purchase, install and test (1) Reduced Size EDS for Terminal Main.	\$0.50	P-Jan I-Mar
CHS	Purchase, install and test (3) Reduced Size EDS for Terminal Main.	\$1.52	P-Jan I-Feb
CMI	Purchase, install and test (1) Reduced Size EDS for Terminal Main.	\$0.50	P-Jan I-Apr
SUN	Purchase, install and test (1) Reduced Size EDS for Terminal Main.	\$0.50	P-Jan I-Apr
GUC	Purchase, install and test (1) Reduced Size EDS for Terminal Main.	\$0.50	P-Mar I-May
SAN-RS	Purchase, install, integrate, network and test (5) Reduced Size EDS for Terminal 1.	\$2.70	P-Jan I-Apr
PHL-RS	Purchase, install, integrate, network and test (3) Reduced Size EDS for Terminal B/C.	\$2.16	P-Mar I-May
HDN	Install, integrate, network and test (3) Reduced Size EDS for Terminal Main.	\$1.24	P-Mar I-May
EGE	Purchase, install, integrate, network and test (2) Reduced Size EDS for Terminal Main.	\$1.56	P-Mar I-Jun
ASE	Purchase, install, integrate, network and test (2) Reduced Size EDS for Terminal Main.		Project canceled and replaced with SBA
SBA	Purchase, install, integrate, network and test (2) Reduced Size EDS for Terminal Main.	\$1.56	P-Mar I-Jul
TUS	Purchase, install, integrate, network and test (4) Reduced Size EDS for Terminal Main.	\$2.02	P-Jan I-Mar
UTA	Purchase, install, integrate, network and test (1) Reduced Size EDS for Terminal Main.	\$0.50	P-Mar I-Jun
RDM	Purchase, install, integrate, network and test (3) Reduced Size EDS for Terminal Main.	\$1.56	P-Jan I-Feb

P = purchase

I = install

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

DEVIATION FROM ORIGINAL SPEND PLAN

After further evaluation, it was determined the current configuration at the Aspen-Pitkin County/Sardy Field (ASE) airport was sufficient to support the needs of the airport. The passenger throughput did not increase as anticipated. The Santa Barbara Municipal (SBA) airport was identified as an airport with increased throughput and served as a replacement airport for the ASE project. The equipment purchase and installation at SBA was comparable to ASE and there were no significant funding changes. The project timeline and schedule were also closely aligned and caused no changes to the current spend plan.

Airport	Technology Purchases	Project Cost \$ in Millions	Planned Obligation Date
N/A	Medium Throughput GE-March–Sept. L3-September	\$84.74	Mar–Sept
N/A	Reduced Size Reveal-Jan–Sept L3-September	\$23.00	Jan–Sept

Airport	Scope of Work	Project Cost \$ in millions	Planned Obligation Date
New Facility Modification Agreement Projects			
ORD	OTA funding for the airport to construct a CBIS for Terminal 1-B South.	\$19.8	May 2009
ICT	OTA funding for the airport to construct a CBIS for Terminal Main.	\$8.25	Sep 2009
SAT	OTA funding for the airport to construct a CBIS for Terminal 1/B.	\$24.0	Sep 2009
FAT	OTA funding for the airport to construct a CBIS for Terminal Main.	\$3.75	Jun 2009
MSP	OTA funding for the airport to construct a CBIS for the Lindbergh Terminal.	\$8.0	Sep 2009
TRI	OTA funding for the airport to construct a CBIS for Terminal Main.	\$3.25	Sep 2009
AMA	OTA funding for the airport to construct a CBIS for Terminal Main.	\$8.25	Sep 2009
PFN	OTA funding for the airport to construct a CBIS for New Terminal.	\$7.25	Sep 2009
Technology/Engineering Initiatives			
N/A	COTR Initiatives, STIP, ASP, OI and Engineering Initiatives	\$40.0	Ongoing thru Sept

*Funding provided in FY 2008

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix F: EBSP Milestones

Project Timelines – New Facility Modification Agreement Projects

Project Timelines – LOI Projects

Major Milestones	Estimated Completion Date
La Guardia (LGA)	
Initiate second year of LOI evaluation	Dec 2008
Airports submit updated cost information to TSA	Apr 2009
Modify existing LOI for additional funding requirements*	May 2009
Newark Liberty International (EWR)	
Initiate second year of LOI evaluation	Dec 2008
Airports submit updated cost information to TSA	Apr 2009
Modify existing LOI for additional funding requirements*	May 2009
John F. Kennedy (JFK)	
Initiate second year of LOI evaluation	Dec 2008
Airports submit updated cost information to TSA	Apr 2009
Modify existing LOI for additional funding requirements*	May 2009

*LOIs require Congressional notification 3 days prior to contract execution.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Project Timelines – EDS Purchase and Install Projects

Major Milestones	Estimated Completion Date
Newark Liberty International (EWR)	
EDS Deliver	Oct 2009
Installation & Integration	Oct 2009
IV&V/ Commissioning	Mar 2010
Live Bag Screening	Apr 2010
Decommissioning	May 2010
Chicago O'Hare International (ORD)	
EDS Delivery	Dec 2009
Installation & Integration	Dec 2009
IV&V/ Commissioning	Apr 2010
Live Bag Screening	May 2010
Decommissioning	Jun 2010
Cincinnati/Northern Kentucky International (CVG)	
EDS Delivery	Feb 2009
Installation & Integration	Aug 2009
IV&V/ Commissioning	Jan 2010
Live Bag Screening	Feb 2010
Decommissioning	Mar 2010
Orlando International (MCO)	
EDS Delivery	Feb 2009
Installation & Integration	Aug 2009
IV&V/ Commissioning	Jan 2010
Live Bag Screening	Feb 2010
Decommissioning	Mar 2010
Miami International (MIA)	
EDS Delivery	Mar 2009
Installation & Integration	Sep 2009
IV&V/ Commissioning	Feb 2010
Live Bag Screening	Mar 2010
Decommissioning	Apr 2010
George Bush Intercontinental/Houston (IAH)	
EDS Delivery	Dec 2009
Installation & Integration	Dec 2009
IV&V/ Commissioning	Mar 2010
Live Bag Screening	Apr 2010
Decommissioning	May 2010

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Project Timelines – EDS Purchase and Install Projects - Continued

Major Milestones	Estimated Completion Date
Nantucket Memorial (ACK)	
EDS Delivery	Feb 2009
Installation & Integration	Feb 2009
Decommissioning	N/A
San Antonio International (SAT)	
EDS Delivery	Oct 2009
Installation & Integration	Oct 2009
IV&V/ Commissioning	Jun 2010
Live Bag Screening	Jul 2010
Decommissioning	Aug 2010
Panama city-Bay County International (PFN)	
EDS Delivery	Dec 2009
Installation & Integration	Dec 2009
IV&V/ Commissioning	Apr 2010
Live Bag Screening	May 2010
Decommissioning	Jun 2010
Norman Y. Mineta San Jose International (SJC)	
EDS Delivery	Jul 2009 & Dec 2009
Installation & Integration	Jul 2009 & Jan 2010
IV&V/ Commissioning	Jan 2010 & Jul 2010
Live Bag Screening	Feb 2010 & Aug 2010
Decommissioning	Mar 2010 & Sep 2010
Rick Husband Amarillo International (AMA)	
EDS Delivery	May 2009
Installation & Integration	May 2009
Decommissioning	N/A
Rogue Valley International-Medford (MFR)	
EDS Delivery	Feb 2009
Installation & Integration	Aug 2009
Decommissioning	N/A
Tallahassee Regional (TLH)	
EDS Delivery	Oct 2009
Installation & Integration	Nov 2009
IV&V/ Commissioning	Apr 2010
Live Bag Screening	May 2010
Decommissioning	Jun 2010

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Project Timelines – EDS Purchase and Install Projects – Continued

Major Milestones	Estimated Completion Date
Kahului (OGG)	
EDS Delivery	Feb 2009
Installation & Integration	Aug 2009
IV&V/ Commissioning	Jan 2010
Live Bag Screening	Feb 2010
Decommissioning	Mar 2010
Phoenix Sky Harbor International Airport (PHX)	
EDS Delivery	Feb 2009
Installation & Integration	Aug 2009
IV&V/ Commissioning	Jan 2010
Live Bag Screening	Feb 2010
Decommissioning	Mar 2010
Pensacola Regional (PNS)	
EDS Delivery	Jan 2009
Installation & Integration	Jul 2009
Decommissioning	Mar 2010
Raleigh-Durham International (RDU)	
EDS Delivery	Oct 2009
Installation & Integration	Mar 2010
IV&V/ Commissioning	Aug 2010
Live Bag Screening	Sep 2010
Decommissioning	Oct 2010
Reno/Tahoe International (RNO)	
EDS Delivery	Jul 2009
Installation & Integration	Aug 2009
Decommissioning	N/A
Greater Rochester International (ROC)	
EDS Delivery	May 2009
Installation & Integration	May 2009
Decommissioning	N/A
San Diego International (SAN)	
EDS Delivery	Feb 2009
Installation & Integration	Aug 2009
IV&V/ Commissioning	Jan 2010
Live Bag Screening	Feb 2010
Decommissioning	Mar 2010

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Project Timelines – EDS Purchase and Install Projects – Continued

Major Milestones	Estimated Completion Date
San Francisco International (SFO)	
EDS Delivery	Dec 2009
Installation & Integration	Jan 2010
IV&V/ Commissioning	Feb 2010
Live Bag Screening	Mar 2010
Decommissioning	Apr 2010
John Wayne Airport-Orange County (SNA)	
EDS Delivery	Nov 2009
Installation & Integration	Nov 2009
IV&V/ Commissioning	Apr 2010
Live Bag Screening	May 2010
Decommissioning	Jun 2010
La Crosse Municipal (LSE)	
EDS Delivery	May 2009
Installation & Integration	May 2009
Decommissioning	N/A
Pittsburgh International (PIT)	
EDS Delivery	Aug 2009
Installation & Integration	Aug 2009
Decommissioning	N/A
Santa Maria Public Airport (SMX)	
EDS Delivery	Jun 2009
Installation & Integration	Jun 2009
Decommissioning	N/A
Hilo International (ITO)	
EDS Delivery	Jun 2009
Installation & Integration	Jun 2009
Decommissioning	N/A
Glacier Park International (GPI)	
EDS Delivery	Jun 2009
Installation & Integration	Jun 2009
Decommissioning	N/A
Molokai Airport (MKK)	
EDS Delivery	Jun 2009
Installation & Integration	Jun 2009
Decommissioning	N/A

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Project Timelines – EDS Purchase and Install Projects – Continued

Major Milestones	Estimated Completion Date
Helena Regional (HLN)	
EDS Delivery	Jun 2009
Installation & Integration	Jun 2009
Decommissioning	N/A
Lovell Field (CHA)	
EDS Delivery	Mar 2009
Installation & Integration	Mar 2009
Decommissioning	N/A
Charleston AFB/International (CHS)	
EDS Delivery	Feb 2009
Installation & Integration	Feb 2009
Decommissioning	N/A
University of Illinois-Willard (CMI)	
EDS Delivery	Apr 2009
Installation & Integration	Apr 2009
Decommissioning	N/A
Friedman Memorial (SUN)	
EDS Delivery	Apr 2009
Installation & Integration	Apr 2009
Decommissioning	N/A
Gunnison-Crested Butte Regional (GUC)	
EDS Delivery	May 2009
Installation & Integration	May 2009
Decommissioning	N/A
San Diego International (SAN-RS)	
EDS Delivery	Apr 2009
Installation & Integration	Apr 2009
Decommissioning	N/A
Philadelphia International (PHL)	
EDS Delivery	May 2009
Installation & Integration	May 2009
Decommissioning	N/A
Yampa Valley (HDN)	
EDS Delivery	May 2009
Installation & Integration	May 2009
Decommissioning	N/A
EDS Delivery	Jun 2009

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Project Timelines – EDS Purchase and Install Projects – Continued

Major Milestones	Estimated Completion Date
Eagle County Regional (EGE)	
EDS Delivery	Jun 2009
Installation & Integration	Jun 2009
Decommissioning	N/A
Aspen-Pitkin County/Sardy Field (ASE)	
EDS Delivery	Project canceled
Installation & Integration	Replaced with SBA
Decommissioning	
Santa Barbara Municipal (SBA)	
EDS Delivery	Jun 2009
Installation & Integration	Jul 2009
Decommissioning	N/A
Tucson International (TUS)	
EDS Delivery	Mar 2009
Installation & Integration	Mar 2009
Decommissioning	N/A
Tunica Municipal (UTA)	
EDS Delivery	Jun 2009
Installation & Integration	Jun 2009
Decommissioning	N/A
Roberts Field (RDM)	
EDS Delivery	Feb 2009
Installation & Integration	Feb 2009
Decommissioning	N/A

Stand-alone EDS equipment is tested at time of delivery. The EDS equipment is usually operational 1 week after installation and testing. Stand-alone equipment only requires decommissioning when a replacement is delivered. When additional units are delivered, no decommissioning is necessary.

An airport's construction schedule generally affects the delivery of the TSA equipment and is out of the control of TSA. When an airport construction schedule slips, delivery timelines are adjusted accordingly.

Airport accepts delivery of equipment depending on construction schedule. The equipment is typically not operational for another 3–6 months for inline systems and 1 week for stand-alone EDS equipment after installation, depending on airport's schedule. TSA awards a delivery order to the Original Equipment Manufacturer (OEM) for services.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Project Timelines – New Facility Modification Agreement Projects

Major Milestones	Estimated Completion Date
Chicago O'Hare International (ORD)	
Notification Letter sent to Airport	February 10, 2009
Draft OTA sent to Airport to review of the terms and conditions	March 22, 2009
Airports submit updated cost information to TSA	February 19, 2009
Cost validations updated based on information provided by the airport.	April 3, 2009
Negotiation meetings scheduled with the airport	April 28, 2009
Negotiations completed and OTA executed	May 2009
Wichita Mid-Continent (ICT)	
Notification letter sent to Airport	February 10, 2009
Draft OTA sent to Airport to review of the terms and conditions	March 22, 2009
Airports submit updated cost information to TSA	February 27, 2009
Cost validations updated based on information provided by the airport.	Late April 2009
Negotiation meetings scheduled with the airport	June 2009
Negotiations completed and OTA executed	September 2009
San Antonio International (SAT)	
Notification Letter sent to Airport	February 10, 2009
Draft OTA sent to Airport to review of the terms and conditions	March 22, 2009
Airports submit updated cost information to TSA	April 10, 2009
Cost validations updated based on information provided by the airport.	April 17, 2009
Negotiation meetings scheduled with the airport	Late May 2009
Negotiations completed and OTA executed	September 2009

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Project Timelines – New Facility Modification Agreement Projects (Continued)

Major Milestones	Estimated Completion Date
Fresno Yosemite International (FAT)	
Notification letter sent to Airport	February 23, 2009
Draft OTA sent to Airport to review of the terms and conditions	February 9, 2009
Airports submit updated cost information to TSA	February 11, 2009
Cost validations updated based on information provided by the airport.	March 31, 2009
Negotiation meetings scheduled with the airport	May 2009
Negotiations completed and OTA executed	June 2009
Minneapolis-St Paul International/Wold-Chamberlain (MSP)	
Notification Letter sent to Airport	February 10, 2009
Draft OTA sent to Airport to review of the terms and conditions	March 22, 2009
Airports submit updated cost information to TSA	April 1, 2009
Cost validations updated based on information provided by the airport.	April 3, 2009
Negotiation meetings scheduled with the airport	June 2009
Negotiations completed and OTA executed	September 2009
Tri-Cities Regional TN/VA (TRI)	
Notification Letter sent to Airport	February 10, 2009
Draft OTA sent to Airport to review of the terms and conditions	March 13, 2009
Airports submit updated cost information to TSA	Late March 2009
Cost validations updated based on information provided by the airport.	April 9, 2009
Negotiation meetings scheduled with the airport	April 28, 2009
Negotiations completed and OTA executed	September 2009

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Project Timelines – New Facility Modification Agreement Projects (Continued)

Major Milestones	Estimated Completion Date
Rick Husband Amarillo International (AMA)	
Notification letter sent to Airport	February 10, 2009
Draft OTA sent to Airport to review of the terms and conditions	April 6, 2009
Airports submit updated cost information to TSA	February 24, 2009
Cost validations updated based on information provided by the airport.	March 25, 2009
Negotiation meetings scheduled with the airport	April 28, 2009
Negotiations completed and OTA executed	September 2009
Panama City-Bay County International (PFN)	
Notification Letter sent to Airport	February 9, 2009
Draft OTA sent to Airport to review of the terms and conditions.	February 9, 2009
Airports submit updated cost information to TSA	March 20, 2009
Cost validations updated based on information provided by the airport.	April 9, 2009
Negotiation meetings scheduled with the airport	June 2009
Negotiations completed and OTA executed	September 2009

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

**Appendix G: Actual vs. Anticipated Unobligated Balance
(as of 3/31/2009)**

Spend Plan Category	Budgeted	Obligated	Unobligated	Anticipated Unobligated
Program Operations and Management	\$74.9	\$15.4	\$59.5	\$0.2
LOI	\$200.0	\$0.0	\$200.0	\$0.0
Other Transactional Agreement (OTA) - New Facility Modification Agreement Projects	\$82.5	\$0.0	\$82.5	\$0.0
EDS Purchase and Install	\$146.6	\$22.6	\$124.0	\$0.0
Technology/Engineering Initiatives	\$40.0	\$3.1	\$36.9	\$3.8
Total	\$544.0	\$41.1	\$502.9	\$4.0

*Anticipated unobligated amounts are payroll accrual and Technology/Engineering initiatives which will not be awarded this fiscal year because of delay in specification designs.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY



Checkpoint Support and Explosive Detection Systems (EDS) Expenditure Plans

Fiscal Year 2009 Report to Congress

Third Quarter Update

November 12, 2009



Homeland
Security

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with

FOR OFFICIAL USE ONLY

Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Message from the Acting Administrator

November 12, 2009

I am pleased to present the "Checkpoint Support and Explosives Detection Systems (EDS) Expenditure Plans" update, which has been prepared by the Transportation Security Administration.

This quarterly report was required by the Fiscal Year 2009 Department of Homeland Security Appropriations Act (P.L. 110-329) and the accompanying Explanatory Statement and Senate Report 110-396. It provides an expenditure plan update for the procurement and installation of emerging technologies and advanced threat detection systems for airport passenger checkpoints and for the procurement and installation of EDS equipment. The report also includes updates on the use of funds provided by the American Recovery and Reinvestment Act (P.L. 111-5).

This report is being provided to the following Members of the Appropriations Committees:

The Honorable Robert C. Byrd
Chairman, Senate Appropriations Subcommittee on Homeland Security

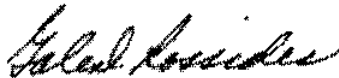
The Honorable George V. Voinovich
Ranking Member, Senate Appropriations Subcommittee on Homeland Security

The Honorable David E. Price
Chairman, House Appropriations Subcommittee on Homeland Security

The Honorable Harold Rogers
Ranking Member, House Appropriations Subcommittee on Homeland Security

If I may be of further assistance, please do not hesitate to contact me at (571) 227-2845 or the Department's Acting Chief Financial Officer, Peggy Sherry, at (202) 447-5751.

Sincerely yours,



Gale D. Rossides
Acting Administrator

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Executive Summary

The Fiscal Year (FY) 2009 Department of Homeland Security Appropriations Act (P.L. 110-329) and the accompanying Explanatory Statement and Senate Report 110-396 requires the Transportation Security Administration (TSA) to submit quarterly updates on Explosive Detection Systems (EDS) and checkpoint expenditures. Checkpoint support funding is implemented through the Passenger Screening Program (PSP). TSA's checked baggage EDS purchase and installation funding is implemented through the Electronic Baggage Screening Program (EBSP).

Checkpoint Support

- PSP tests, procures, deploys, integrates, and provides life cycle support for security equipment to screen passengers and carry-on baggage at passenger checkpoint lanes at domestic airports. PSP is responsible for technologies that screen more than 700 million passengers per year at approximately 450 of the Nation's airports.
- The Advanced Surveillance Program (ASP) utilizes the existing infrastructure owned and operated by the transportation authority for remote monitoring, threat detection and assessment in a partnership agreement to provide enhanced situational awareness.
- Major updates in the third quarter include the following:
 - An additional \$11.1 million of American Recovery and Reinvestment Act (ARRA) funds added to checkpoint support for ASP/Closed Circuit Television (CCTV) projects
 - \$7 million included for Chemical Analyzer Detectors
 - \$18 million included for Credential Authentication Technology

Electronic Baggage Screening Program

- The EBSP oversees the screening of all baggage checked in airports nationwide. EBSP tests, procures, deploys, integrates and provides life cycle support for approximately 7,700 pieces of security equipment that screen checked baggage at approximately 450 of the Nation's airports.
- The EBSP allocates resources to airport baggage screening facility modification projects, purchase and installation of EDS technology and technology initiatives aimed at improving operational effectiveness and efficiencies, as well as the programmatic resources required to ensure effective execution of the program.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

- Major updates in the third quarter include the following:
 - FY 2009 funds were reallocated from Engineering Initiatives for the purchase of the TSA Systems Integration Facility building.
 - Through cost validation and negotiation, TSA was able to reduce projected costs for EDS airport projects from the original ARRA expenditure plan by almost \$310 million. Ten additional airports were added to the spend plan, and \$11.1 million was transferred from the EDS ARRA funds to finance checkpoint support for ASP/CCTV projects.
 - \$38.4 million of the EDS funds will be used for ASP/CCTV projects in the checked baggage area of the airport.
 - An additional \$30 million of the EDS funds will be used to procure and install Reduced Size EDSs to Explosives Trace Detection (ETD)-only airports to improve operational efficiencies and screening effectiveness.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY



Checkpoint Support and Explosives Detection Systems (EDS) Expenditure Plans 3rd Quarter Update, Fiscal Year 2009

Table of Contents

I. Legislative Requirement.....	1
II. Passenger Screening Program (PSP)	2
A. Background	2
B. Expenditure Plan	4
C. Program Initiatives.....	6
III. Electronic Baggage Screening Program (EBSP).....	13
A. Background	13
B. Expenditure Plan	16
IV. Appendices.....	23
Appendix A. Abbreviations/Acronyms	23
Appendix B. Airport Codes.....	25
Appendix C. Passenger Screening Program (PSP) Deployments by Airport	31
Appendix D. PSP FY 2009 Summary Spend Plan	35
Appendix E. PSP American Recovery and Reinvestment Act (ARRA) Summary Spend Plan	38
Appendix F. PSP FY 2009 Obligation Data	40
Appendix G. PSP ARRA Obligation Data	41
Appendix H. PSP FY 2009 Milestones	42

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix I. PSP ARRA Milestones	43
Appendix J. PSP FY 2009 Actual vs. Anticipated Unobligated Balance, as of June 30, 2009	45
Appendix K. PSP ARRA Actual vs. Anticipated Unobligated Balance, as of June 30, 2009	46
Appendix L. Electronic Baggage Screening Program (EBSP) FY 2009 Obligation by Project	47
Appendix M. EBSP ARRA Obligation by Project	50
Appendix N. EBSP FY 2009 Summary Spend Plan	51
Appendix O. EBSP ARRA Summary Spend Plan	59
Appendix P. EBSP FY 2009 Obligation Data	68
Appendix Q. EBSP ARRA Obligation Data	76
Appendix R. EBSP FY 2009 Milestones	77
Appendix S. EBSP ARRA Milestones	88

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

I. Legislative Requirement

The Fiscal Year (FY) 2009 Department of Homeland Security (DHS) Appropriations Act (P.L. 110-329) and the accompanying Explanatory Statement and Senate Report 110-396, includes the following requirement:

Aviation Security—Explosive Detection Systems

TSA shall provide an expenditure plan to the Committees not later than 60 days after the date of enactment of this Act, as discussed under Transportation Security Support. If new requirements occur after the plan is submitted, TSA shall reassess and reallocate funds after notifying the Committees of any change. As discussed in the Senate report, TSA shall provide quarterly updates on EDS and checkpoint expenditures, on an airport-by-airport basis. These updates shall include information on the specific technologies for purchase, project timelines, a schedule for obligation, and a table detailing actual versus anticipated unobligated balances at the close of the fiscal year, with an explanation of any deviation from the original plan.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

II. Passenger Screening Program (PSP)

A. Background

Mission

PSP's Mission Need supports prevention and protection from terrorist and criminal actions in the aviation transportation environment. PSP specifically focuses on technology and processes utilized in and near the passenger screening checkpoint to achieve the air travel passenger security mission. PSP's mission includes being responsible for the acquisition of technology that identifies threats concealed on people and their carry-on items entering the sterile area of the airport terminal through the passenger screening checkpoint. The checkpoint is defined as the screening equipment, processes and operating personnel collectively required to perform the security mission.

Purpose

PSP accomplishes its mission by identifying, testing, procuring, deploying, integrating and sustaining equipment that identifies threats concealed on passengers and their carry-on items as they enter the airport terminal through the passenger screening checkpoint.

Goals

PSP supports Goal One of the DHS Strategic Plan, FY 2008-2013, "Protect Our Nation from Dangerous People."

PSP Objectives:

- **Explosives Detection:** Detect explosives threats, weapons and other prohibited items concealed on passengers and their carry-on items.
- **Screening Efficiency:** Improve checkpoint efficiency through process automation.
- **Layered Security:** Enable a layered, integrated security solution.

The following are accomplishments of PSP technologies:

- **Advanced Technology (AT) X-Ray.** More than 850 AT (first-generation) operational units deployed nationwide have expanded the capabilities of the Transportation Security Officers (TSOs) at the checkpoint; these units replace legacy Threat Image Projection (TIP) Ready X-Ray (TRX) systems. AT systems are penetration x ray-based technologies that provide an enhanced view of a bag's contents through improved image resolution. Also, an added dimension to the displayed image provides better material discrimination for TSOs to discern each object inside a bag. AT systems are

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

upgradeable, offering a cost-effective platform to develop enhanced detection capabilities. Additionally, AT systems can include the universal conveyor system (UCS), which diverts bags requiring a secondary search. The UCS will assist in maintaining positive control of and tracking all passenger carry-on baggage until the screening technology clearly indicates the baggage's status and a TSO decides to deliver the baggage to the passenger. This functionality will improve overall throughput and minimize congestion on the exit side of the AT system. Deployments are ongoing and the second generation of AT will undergo testing in the fourth quarter of FY 2009.

- **Advanced Imaging Technology (AIT).** Previously known as whole body imaging or WBI, AIT is a new imaging capability that will be used to inspect a passenger for concealed weapons (metal and non-metal), explosives and other prohibited items. In addition, the AIT offers operators the opportunity to review anomalies on an individual to determine if a physical pat-down inspection is required. AITs could ultimately be the primary passenger screening technology instead of using an Enhanced Metal Detector (EMD). The Transportation Security Administration (TSA) has assessed two types of technologies for the AITs, including x ray backscatter and millimeter wave technology. Both offer safe and effective screening for weapons and explosives concealed on a person. Deployments are ongoing and the second generation of AIT will undergo testing in the fourth quarter of FY 2009.
- **Bottled Liquid Scanner (BLS).** A BLS offers detection capability that can discriminate explosives or flammable liquids from common, benign liquids carried by passengers. The device analyzes substances within a container (bottle or can), measuring particular characteristics of the contents and distinguishing between benign and hazardous liquids in seconds. The second-generation devices perform scans without breaking seals or contaminating passengers' property and will greatly reduce annual consumable costs.
- **Credential Authentication Technology/Boarding Pass Scanning Systems (CAT/BPSS).** CAT/BPSS provides a common platform for automated credential authentication and boarding pass validation. First-generation systems will allow the TSA to verify that forms of identification presented to gain access to sterile areas in airports are genuine documents and that boarding passes have been issued by a valid airline and no tampering with the data stored on the boarding pass has occurred. Second-generation systems will allow the TSA to compare data from passengers' identification to data stored in the 2D barcode on the boarding pass. Second-generation systems will also feature an expanded library of airport, airline and law enforcement identification. CAT/BPSS units will provide the TSA with increased control of access to airport sterile areas. CAT/BPSS recently completed pilot programs at Ronald Reagan Washington National Airport and Baltimore/Washington International Thurgood Marshall Airport as part of the current solicitation.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

- **Chemical Analyzer Detector (CAD).** CADs will be used to assess suspicious substances in the possession of people passing through security checkpoints. Bomb Appraisal Officers (BAOs) will respond to requests by screener personnel for advanced alarm resolution (that is, secondary offline screening) of liquids, powders and solid suspicious substances at the airport and other designated security checkpoints.

The following chart shows enacted amounts since inception of the Checkpoint Support Program, Project and Activity (PPA). Values are in millions of dollars.

2002	2003	2004	2005	2006	2007	07 supp	2008	2009	ARRA	TOTAL
\$ 38.00	\$ 40.00	\$ 61.86	\$ 123.60	\$ 164.00	\$ 173.37	\$ 25.00	\$ 250.00	\$ 245.20	\$ 311.15	\$ 1,432.08

B. Expenditure Plan

Summary of PSP Expenditure Plan (dollar amounts in millions)

Section	FY09 Approved	ARRA Approved	Total Approved	FY09 Revised	ARRA Revised	Total Revised
Technology	\$ 149.70	\$ 197.70	\$ 347.40	\$ 113.10	\$ 202.90	\$ 316.00
Program Operations and Management	\$ 35.70	\$ 82.90	\$ 118.60	\$ 63.50	\$ 77.70	\$ 141.20
Technical and Engineering Initiatives	\$ 22.60	\$ 9.90	\$ 32.50	\$ 26.60	\$ 9.90	\$ 36.50
Safety and Optimization	\$ 13.50	\$ -	\$ 13.50	\$ 13.50	\$ -	\$ 13.50
Checkpoint Reconfiguration	\$ 11.50	\$ -	\$ 11.50	\$ 11.50	\$ -	\$ 11.50
Advanced Surveillance Program	\$ 11.00	\$ 5.70	\$ 16.70	\$ 11.00	\$ 16.85	\$ 27.85
Personnel Compensation and Benefits	\$ 6.00	\$ 3.80	\$ 9.80	\$ 6.00	\$ 3.80	\$ 9.80
Total	\$ 250.00	\$ 300.00	\$ 550.00	\$ 245.20	\$ 311.15	\$ 556.35

FY09 Revised: Total lower due to funds being reallocated to another PPA.

ARRA Revised: Total higher, additional airports to be served by ASP

FY 2009 reallocations were necessary to account for additional integration requirements of the emerging technologies. American Recovery and Reinvestment Act of 2009 (ARRA) changes include the addition of the CADs, CAT and airports for the Advanced Surveillance Program (ASP). UCS was lowered by approximately 50 units to account for added integration requirements and to procure additional explosives trace detectors.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Technology Purchases and Percentages to Reach Full Operational Capability (FOC)

Technology	FOC	Purchases with Prior Year Funds	Prior Years	Purchases with FY09 Funds	FY09	Purchases with ARRA Funds	ARRA	PURCHASES TOTAL	TOTAL % of FOC
Advanced Technology ¹	2325	1029	44%	485	6%	613	92%	2128	91%
Universal Conveyor Systems	2325	0	0%	0	0%	238	10%	238	10%
Advanced Imaging Technology	878	47	5%	175	25%	200	45%	422	48%
Credential Authentication Technology	2325	0	0%	0	0%	500	34%	500	21%
Bottled Liquids Scanners	1500	200	13%	600	62%	500	100%	1300	100%
Explosives Trace Detectors	1500	100	7%	0	7%	400	33%	500	33%
Chemical Analyzer Detector	140	0	0%	0	0%	140	100%	140	100%

¹ Percentage of FOC based on FY14 estimates

Checkpoint Support Expenditure Plan

PROGRAM SPENDING PLAN: Checkpoint Support

APPROPRIATIONS IN \$ MILLIONS

Net Appropriated Funds	856.360
Funds Obligated	35.807
Project Outlays	7.441
Unobligated Balance	820.843

UNOBLIGATED BALANCES BY FY

FY08/ARRA	Total
520.843	520.843

OBLIGATIONS IN \$ MILLIONS

	Q1FY08	Q2FY08	Q3FY08	Q4FY08	FY10	FY11	FY12	FY13	FY14
Plan	16.280	40.280	218.510	278.410	4.880	-	-	-	-
Plan Cumulative	16.280	56.560	275.050	551.460	556.360	-	-	-	-
Cumulative % Allotment	0.00%	21.81%	12.21%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Actual	-	8.825	26.682	-	-	-	-	-	-

OUTLAYS IN \$ MILLIONS

	Q1FY08	Q2FY08	Q3FY08	Q4FY08	FY10	FY11	FY12	FY13	FY14
Plan	-	8.000	22.850	54.270	480.430	-	-	-	-
Plan Cumulative	-	8.000	30.850	84.920	565.360	-	-	-	-
Cumulative % Allotment	0.00%	24.79%	22.77%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Actual	-	1.983	5.158	-	-	-	-	-	-

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

C. Program Initiatives

Description of Initiative I – AT X-Ray

- AT systems are penetration x ray-based technologies that provide an enhanced view of a bag's contents through improved image resolution beyond the capabilities of the currently fielded TRX equipment. Also, an added dimension to the displayed image provides better material discrimination for TSOs to discern each object inside a bag. AT offers a cost-effective platform to develop enhanced detection capabilities. Future enhancements may include an enhanced conveyor system. More than 850 first-generation AT units are being deployed and installed at airports nationwide. The second generation of AT with upgraded capability and functionality is in the development stage.
- Obligations to date: \$106.6 million
- Projected FY 2009 obligations by year: FY 2009 – \$0, FY 2010 – \$61.0 million
- Projected FY 2009 expenditures: FY 2010 – \$61.0 million
- Projected ARRA obligations by year: FY 2009 – \$2.9M, FY 2010 – \$73.5 million
- Projected ARRA expenditures by year: FY 2009 – \$2.9 million, FY 2010 – \$73.5 million
- Major performance objectives:
 - Probability of detection of threat items: Classified
 - Throughput: ≥ 440 bags per hour with operator intervention
 - Operational availability: ≥ 98 percent
- Activities and milestones/accomplishments:
 - Initial Operational Capability (IOC): Q3 FY 2008
 - Qualification Testing and Evaluation (QT&E): Q4 FY 2009
 - Operational Testing and Evaluation (OT&E): Q4 FY 2009
 - Contract award: Q1 FY 2010
 - FOC: Q1 FY 2011 accelerated from Q2 FY 2014

Description of Initiative II – UCS

- UCSs are carry-on baggage handling conveyor systems added to the AT systems to support automated diversion of alarm bags from cleared baggage.
- Obligations to date: \$0
- Projected ARRA obligations: FY 2010 – \$28.5 million
- Projected ARRA expenditures by year: FY 2010 – \$8.5M, FY 2011 – \$20.0 million
- Activities and milestones/accomplishments:
 - Contract award: Q2 FY 2010
 - IOC: Q2 FY 2010

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Description of Initiative III – AIT

- AIT provides an imaging capability used to inspect a passenger's body for concealed weapons (metal and nonmetal), explosives and other prohibited items in place of a metal detection wand inspection and physical pat-down. The AIT could potentially become a primary screening technology, which could be used in conjunction with, or instead of, an EMD.
- Obligations to date: \$13.6 million
- Projected FY 2009 obligations: FY 2009 – \$28.9 million
- Projected FY 2009 expenditures: FY 2010 – \$28.9 million
- Projected ARRA obligations: FY 2009 – \$32.2 million
- Projected ARRA expenditures: FY 2010 – \$32.2 million
- Major performance objectives:
 - Probability of threat detection: Classified
 - Throughput: ≥ 200 passengers per hour
 - Operational availability: ≥ 98 percent
- Activities and milestones/accomplishments:
 - QT&E: Q4 FY 2009
 - OT&E: Q4 FY 2009
 - Contract award: Q4 FY 2009
 - IOC: Q4 FY 2009
 - FOC: Q4 FY 2014

Description of Initiative IV – CAT

- The CAT system provides a primary means for automated verification of passenger travel documents and forms of identification that passengers present to TSOs during the security checkpoint screening process, as well as those forms of identification presented by airport and airline personnel to access sterile areas. This system will increase TSOs' abilities to locate fraudulent IDs and validate the issuing authority and authenticity of boarding passes at security checkpoints.
- Obligations to date: \$0
- Projected ARRA obligations: FY 2009 – \$18.0 million
- Projected ARRA expenditures: FY 2010 – \$18.0 million
- Activities and milestones/accomplishments:
 - Request for proposals: Q3 FY 2009
 - Contract award: Q4 FY 2009
 - FOC: Q2 FY 2011

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Description of Initiative V – BLS

- A BLS is an Explosives Detection System (EDS) that differentiate liquid explosives from common, benign liquids. BLS utilize a variety of technologies to detect liquid explosives and explosive precursors, including vapor detection, x ray detection, detection using the dielectric properties of the materials being scanned or optical detection using Raman spectroscopy.
- Obligations to date: \$0
- Projected FY 2009 obligations: FY 2009 – \$22.7 million
- Projected FY 2009 expenditures: FY 2010 – \$22.7 million
- Projected ARRA obligations: FY 2009 – \$18.8 million
- Projected ARRA expenditures: FY 2010 – \$18.8M
- Major performance objectives:
 - Probability of detection of threat items: Classified
 - Throughput: ≥ 180 samples per hour
 - Operational availability: ≥ 98 percent
- Activities and milestones/accomplishments:
 - IOC To Be Determined (TBD): Q1 FY 2010
 - QT&E: Q3 FY 2009
 - OT&E: Q4 FY 2009
 - Contract award: Q4 FY 2009
 - FOC: Q1 FY 2011

Description of Initiative VI – Next Generation (Next Gen) ETD

- Next Gen ETDs identify a larger range of explosives than earlier models. The Next Gen ETDs have enhanced explosives detection capability, including increased sensitivity and the ability to detect new threats. The Mean Time to Repair will be significantly less than for the current ETD technology. In addition, the Next Gen ETDs will have a Field Data Reporting System and will be Security Technology Integration Program capable. Because of these significant improvements, a lower life cycle cost is expected.
- Obligations to date: \$6.1 million
- Projected FY 2009 obligations: FY 2009 – \$0.5 million
- Projected FY 2009 expenditures: FY09 – \$0.5 million
- Projected ARRA obligations: FY 2009 – \$22.0 million
- Projected ARRA expenditures: FY 2010 – \$22.0 million
- Major performance objectives:
 - Probability of detection of threat items: Classified
 - Throughput: 180 samples per hour, to include machine processing and analysis, when no alarms are present
 - Operational availability: ≥ 98 percent
- Activities and Milestones/Accomplishments:
 - QT&E: Q1 FY 2008

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

- OT&E: Q2 FY 2008
- Contract award: Q4 FY 2008
- IOC: Q1 FY 2009
- FOC: Q4 FY 2014

Description of Initiative VII – CADs

- CADs are portable systems that can be used by BAOs and Explosives Security Specialists (ESS) to identify a range of chemical agents, precursors and explosives threats quickly. These devices will be used to assess suspicious substances in the possession of passengers traveling through the security checkpoints.
- Obligations to date: \$0.25 million
- Projected FY 2009 obligations: FY 2009 – \$0
- Projected FY 2009 expenditures: FY 2009 – \$0
- Projected ARRA obligations by year: FY 2009 – \$0.25 million; FY 2010 – \$6.75 million
- Projected ARRA expenditures: FY 2010 – \$7.0 million
- Major performance objectives:
 - Probability of detection of threat items: Classified
 - Operational availability: ≥ 96 percent
- Activities and Milestones/Accomplishments:
 - QT&E: Q4 FY 2009
 - OT&E: Q1 FY 2010
 - Contract award: Q1 FY 2010
 - IOC: Q1 FY 2010
 - FOC: Q4 FY 2010

Description of Initiative VIII – Integration

Relates to all tasks associated with the installation of security technology equipment at geographically dispersed airports nationwide.

- **Integration** services can include moving equipment, small-scale facility modification or electrical and plumbing repairs.
- **Project Logistics** deal with the procurement, distribution and replacement of systems to and from the field.
- **Installation and Design** services encompass architectural design and review, site survey and construction package review.
- Projected FY 2009 obligations: FY 2009 – \$31.9 million
- Projected FY 2009 expenditures by year: FY 2009 – \$15.0 million; FY 2010 – \$16.9 million
- Projected ARRA obligations: FY 2009 – \$68.2 million
- Projected ARRA expenditures: FY 2010 – \$68.2 million

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Description of Initiative IX – Program Operations and Management

Program Operations and Management encompasses activities needed for the procurement and deployment of security systems to the Nation's airports. The following activities make up this initiative:

- **Engineering Support** encompasses requirements review, technical representation and technical management support.
- **Independent Verification and Validation** encompasses factory acceptance testing, site acceptance testing and integrated site testing.
- **Data Collection** activities are those associated with documentation, reports and technical support of testing.
- **TSA Systems Integration Facility** provides an operationally realistic environment to evaluate current/new advanced screening technologies, processes and procedures against known threats to transportation venues, particularly air transportation venues.
- **Program Resource and Data Management** activities encompass project management support, financial management and analysis, data management and project scheduling.
- Projected FY 2009 obligations: FY 2009 – \$31.6 million
- Projected FY 2009 expenditures by year: FY 2009 – \$20.0 million; FY 2010 – \$11.6 million
- Projected ARRA obligations by year: FY 2009 – \$2.0 million, FY 2010 – \$7.5 million
- Projected ARRA expenditures: FY 2010 – \$9.5 million

Description of Initiative X – Technical and Engineering Initiatives

- **Security Technology Integration Program** is an agencywide system that enables TSA to connect all Transportation Security Equipment to one data management system that will facilitate the exchange of information across the network and facilitate maintenance servicing and diagnostic information.
- **Operational Integration (OI) of Emerging Technology** consists of data collection, research and field tests to verify systems, operational innovations and screening upgrades in a variety of conditions, climates and processes. Reliability, maintainability and availability will be assessed on new technologies and innovations so that decisions concerning their deployability and usefulness can be effectively made. Examples of emerging technologies to be field tested and piloted include AIT, AT, BLS and CAT (including passenger wait-time collection pilot).
- **TIP** keeps TSOs alert and exposes them to a variety of prohibited item images they may not normally see. It is also used as an evaluation tool to assess a TSO's visual inspection performance of detecting prohibited items during real working hours instead of in lab conditions.
- **Engineering Changes** are required to modify technology to support enhanced capabilities such as throughput, detection, operator interface, and so on.
- **Exit Lane Breach Control** tests and evaluates the performance capabilities and technical viability of technologies that minimize the risk of unauthorized access and reduce resource requirements at exit lanes.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

- Projected FY 2009 obligations: FY 2009 – \$26.6 million
- Projected FY 2009 expenditures by year: FY 2009 – \$15.0 million; FY 2010 – \$11.6 million
- Projected ARRA obligations: FY 2010 – \$9.9 million
- Projected ARRA expenditures: FY 2010 – \$9.9 million

Description of Initiative XI – Safety and Optimization

- The Safety and Optimization Program improves the safety and efficiency of checkpoints and checked baggage screening operations by deploying ancillary equipment and enhancing the design and layout of screening areas.
- Funding will be used to procure equipment and services to complete airport safety enhancement projects to minimize the amount of TSOs injured on the job.
- Projected FY 2009 obligations: FY 2009 – \$13.5 million
- Projected FY 2009 expenditures by year: FY 2009 – \$9.0 million; FY 2010 – \$4.5 million

Description of Initiative XII – Checkpoint Reconfiguration

- Checkpoint reconfigurations are required at airports to maintain or improve throughput due to the growth in passenger traffic and the evolution of the airline industry. Reconfiguration of checkpoints can also be required as emerging technologies are deployed to efficiently utilize the checkpoint space.
- Funding will be used to procure glass for wand stations, adjustable divest and composure tables and ancillary equipment for checkpoints such as podiums and benches, as well as to reconfigure checkpoint equipment and layouts to accommodate emerging technologies and redesign to make checkpoints more efficient.
- Projected FY 2009 obligations: FY 2009 – \$11.5 million
- Projected FY 2009 expenditures by year: FY 2009 – \$4.0 million, FY 2010 – \$7.5 million

Description of Initiative XIII – ASP

- ASP utilizes the existing infrastructure owned and operated by the transportation authority for remote monitoring, threat detection and assessment in a partnership agreement to provide enhanced situational awareness of the checkpoint and checked baggage area of airports.
- Obligations to date: about \$48.0 million
- Projected FY 2009 obligations: FY 2009 – \$11.0 million
- Projected FY 2009 expenditures: FY 2010 – \$11.0 million
- Projected ARRA obligations: FY 2009 – \$16.8 million
- Projected ARRA expenditures: FY 2010 – \$16.8 million

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

- Activities and Milestones/Accomplishments:
 - Site visits: TBD by airport
 - Proposals: Q3 FY 2009
 - Contract awards: Q4 FY 2009

Description of Initiative XIV – Personnel Compensation and Benefits (PC&B)

- Projected FY 2009 expenditures: FY 2009 – \$6.0 million
- Projected ARRA expenditures: FY 2010 – \$3.8 million

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

III. Electronic Baggage Screening Program (EBSP)

A. Background

Mission

EBSP's mission is central to the TSA security mission area because it covers: *"The range of TSA activities that minimize the risk of injury or death of people or damage or loss of property due to hostile acts of terrorism that may be directed against the National Airspace System."* Preventing catastrophic loss and air piracy involves verifying that checked baggage carries no prohibited items or items that have been identified as threat objects for the particular transportation mode. The screening process targets the checked baggage of all people boarding aircraft through the use of screening security systems.

EBSP tests, acquires, deploys, integrates and maintains the technology that screens passenger-checked baggage to deter, detect, mitigate and prevent transportation of explosives or other prohibited items on commercial aircraft while ensuring freedom of movement for people and commerce.

Purpose

EBSP was initiated by the White House Commission on Aviation Safety and Security at the Federal Aviation Administration in 1997. In response to the events of September 11, 2001, a Congressional mandate transferred the EBSP to DHS. Furthermore, public laws were enacted to accelerate and dramatically increase the scope of the EBSP. The Aviation and Transportation Security Act (ATSA), P.L. 107-71, stated that all checked baggage must be screened at all the nation's airports with an EDS or a suitable alternative as soon as possible but not later than December 31, 2002. The Homeland Security Act of 2002 (HSA), P.L. 107-296, later granted DHS a waiver until December 31, 2003, to screen all checked baggage at all airports, a condition that was met.

EBSP is currently in a "mixed" acquisition life cycle, focusing predominately on the purchase, deployment and sustainment phases of the acquisition process. The primary technologies acquired and deployed under the EBSP are EDS equipment and ETD devices. The following three technology configurations comply with the mandates of ATSA and the HSA:

1. ETD-based Systems – TSOs use ETD machines as a primary method to screen bags.
2. Standalone EDSs – TSOs use EDS machines as a primary method to screen bags. Alarmed bags are resolved by ETDs.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

3. Inline EDS Systems – TSOs use EDS machines as a primary method to screen bags. Alarmed bags are resolved by ETDs.

Using EDS technology (both inline and standalone) is preferred over using ETDs as a primary screening method because of the following:

1. (b)(3)-49 U.S.C. § 114(r) (detailed performance capabilities are classified). Improving security supports TSA and DHS goals to prevent and protect.
2. Increased Efficiency – EDS machines have a higher throughput than ETD units used in primary screening, which decreases lobby congestion and passenger wait time. Higher baggage throughput supports TSA's goal of "ensuring freedom of movement for people and commerce."
3. Decreased Labor Costs – EDS configurations at larger airports require fewer TSOs to operate than ETDs used in primary screening configurations. Increased automation reduces human error and personnel costs. EDS machines also have reduced operating costs over the life of the equipment and require less lifting of baggage, thus reducing the number of on-the-job injuries.

These technologies have been in production since 1997, and production is expected to continue indefinitely with enhancements both to engineering and detection capabilities. EBSF currently manages seven technology vendors and 16 technology models and provides life-cycle procurement, deployment, integration and maintenance of more than 7,700 units of security equipment at approximately 450 U.S. Federalized airports. To date, EBSF has supplied 68 airports with full optimal systems and enabled some screening areas with optimal systems at 52 additional airports.

The following chart shows the enacted/appropriated funding since inception of the EDS/ETD Install and Purchase PPA. Values are in millions of dollars.

Program Project and Activity	2002	02 Supp	2003	03 Supp	2004	2005	2006	2007	07 Supp	2008	2009	APRA	TOTAL
EDS/ETD Purchase	\$959.90	\$0.00	\$174.50	\$3.00	\$150.00	\$180.00	\$175.00	\$141.40	\$55.44	\$100.63	\$107.70	\$50.00	\$2,007.47
EOS/ETD Installation	\$0.00	\$738.00	\$265.00	\$235.00	\$250.00	\$285.00	\$295.00	\$388.00	\$229.56	\$440.37	\$435.30	\$828.85	\$4,201.23
Total	\$959.90	\$738.00	\$439.50	\$238.00	\$400.00	\$475.00	\$470.00	\$529.40	\$285.00	\$540.90	\$543.00	\$878.85	\$6,208.70

* Includes the Aviation Security Capital Fund (ASCF) Fee beginning FY 2007

Goal

The EBSF supports Goal Two of the DHS Strategic Plan, FY 2008-2013, "Protect Our Nation from Dangerous Goods."

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

EBSP fulfills the congressional mandate for 100 percent screening of aviation checked baggage by electronic or other approved means (found in ATSA Section 110).

The mandate to screen 100 percent of checked baggage has been achieved, and ongoing efforts to operate, maintain and improve screening systems remains critical. In particular, it is imperative that the program continue to research, evaluate and deploy refinements to EDS and ETD technology and associated systems that allow for improvements in (1) throughput (checked bags per hour), (2) the false alarm rate, (3) system availability and (4) total cost of ownership for baggage screening (cost per checked bag). In addition, it is desirable to relocate equipment from airport lobby areas to baggage room areas.

Program progress to date relative to EDS/ETD deployment and facility modifications

EDS/ETD Purchases
Historical Funding (FY 2004 through FY 2009)
Dollars in Thousands

	Purchase	Install	Units/EDSs	Units/ETDs	Agreements	% Agreements Awarded*	% Install Awarded**
FY 2004							
Enacted	149,700	249,000	136	24	19	100	100
FY 2005							
Enacted	180,000	295,000	134	248	3	100	100
FY 2006							
Enacted	175,000	295,000	216	552	17	100	100
FY 2007							
Enacted***	141,400	388,000	133	529	7	100	100
FY 2007 Supplemental							
Enacted***	55,440	229,560	48	0	6	100	100
FY 2008							
Enacted***	103,627	440,373	114	3	10	100	95
FY 2009							
Enacted***	107,700	436,300	129	0	11	0	86
ARRA	60,000	628,850	160	0	26	11	28

*Agreements awarded: percent of planned project Other Transactional Agreements (OTAs)/Letters of Intent (LOIs) awarded either in the year funding was appropriated or the following year with carryover funding

**Install awarded: percent of planned airport projects completed with EDS/ETD purchased and installed equipment either in the year funding was appropriated or the following year with the available carryover funding. The FY 2008 planned purchase and installation projects will be completed in FY 2009 with available carryover funding.

***Includes \$250 million Aviation Security Capital Fund fees

Per congressional direction, EBSP allocates funding among a wide variety of airports ranging from non-hub to large. Funding provided to EBSP by the ARRA will reduce the timeline for reaching the optimal solution at all airports by up to 2-3 years. When EBSP nears the achievement of its optimal solution, funding allocation will begin to shift from primarily

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

purchase and install costs to operations and management and recapitalization costs as the need for new installations decreases.

The TSA is currently planning to enter into letters of intent (LOI) negotiations with airports in Los Angeles, CA; Washington, DC; Tallahassee, FL and Fort Lauderdale, FL, for FY 2010. This early communication with the selected airports will ensure that TSA continues with the expedited deployment of EDSs to maintain a high level of system efficiency and effectiveness by decreasing threats.

B. Expenditure Plan

Summary of EBSP Expenditure Plan

Section	FY09 Approved	ARRA Approved	Total Approved	FY09 Revised	ARRA Revised	Total Revised
Program Operations and Management	\$74.9	\$32.0	\$106.9	\$97.5	\$54.85	\$152.35
LOI	\$200.0	\$0.0	\$200.0	\$200.0	\$0.0	\$200.0
OTA/New Facility Modification Agreement Projects	\$82.5	\$598.1	\$680.6	\$67.3	\$499.2	\$566.5
EDS Purchase and Install	\$146.6	\$64.2	\$210.8	\$146.6	\$94.2	\$240.8
Technology/Engineering Initiatives	\$40.0	\$5.7	\$45.7	\$32.6	\$40.6	\$73.2
Total	\$544.0	\$700.0	\$1244	\$544.0	\$688.85	\$1232.85

FY 2009

The FY 2009 Spend Plan totals \$544 million in FY 2009 enacted level:

- Total FY 2009 Purchase Funds equal \$107.7 million of enacted FY 2009 funds
- Total FY 2009 Install Funds equal \$436.3 million, which includes \$186.3 million of enacted FY 2009 funds and \$250 million Airport Security Capital Funds

Total project costs represent incurred costs: original equipment procurement, manufacturer installation, integration, multiplexing, warehousing, shipping, testing and facility modifications.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Facility modification amounts are based on FY 2009 application information and TSA cost validation process. The amount is subject to change because of updated cost submittals and negotiations with the airport.

TSA has identified a total of three LOIs, eight airports for facility modifications and 42 airports for Purchase and Installations.

ARRA

Based on the established long-term EDS Strategic Planning Framework, plus airport-specific project information, EBSP submits a revised ARRA spend plan totaling \$688.85 million for the purchase of EDS equipment, installation of EDS equipment and facility modifications to airports to accommodate the EDS equipment. The original plan was submitted with \$700 million for this program, but further organizational review revealed a need to support ASP and resulted in a reallocation of \$11.15 million to PSP, resulting in a reduction of the EDS allocation.

Total project costs represent the following incurred costs: original equipment procurement, manufacturer installation, integration, multiplexing, warehousing, shipping, testing and facility modifications.

Facility modifications are based on initial applications and the TSA cost validation process. The amount is subject to change because of updated cost submissions and negotiations with the airports.

The 16 airports identified to receive the first infusion of ARRA funds from TSA were selected from a pool of completed applications originally submitted for FY 2009 funding, but which remained unfunded because of resource limitations. The 16 airports had already provided complete applications, enjoyed proactive airport administrations and represented a cross-section of mid- to larger-size airports. Also, when taken together, the 16 airports comprised a significant percentage of passenger traffic, hence yielding excellent security enhancement value for the amount of ARRA funds identified. Of the original 16 airports which agreed to participate, one airport (Tallahassee) has since withdrawn.

The original ARRA spend plan reflected a total cost of about \$598 million for facility modifications, while revised projected costs totaled approximately \$499.2 million. Ultimately, through the process of cost validation and negotiation, TSA was able to reduce the total projected costs for EDS airport projects from the original ARRA spend plan by more than \$80 million while also adding 10 airport projects. The savings achieved will allow the EBSP to improve the security and efficiency of the screening process at these 10 airports, which had cost-validated plans in place but were previously deferred to FY 2010 and beyond.

TSA identified 10 airports as potential candidates for these additional EDS airport projects. All would be able to accept the funding in the accelerated cycle and complete their proposed projects

FOR OFFICIAL USE ONLY

<p>WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.</p>

FOR OFFICIAL USE ONLY

in the allowable time frames. The total cost for the 10 additional airports is \$243 million. The 10 additional airports are:

- Lambert-Saint Louis International, St. Louis, MO
- Washington Dulles International, Chantilly, VA
- Yellowstone Regional, Cody, WY
- William P. Hobby, Houston, TX
- St. Petersburg-Clearwater International, St. Petersburg, FL
- Gallatin Field, Bozeman, MT
- Little Rock National, Little Rock, AR
- Tulsa International, Tulsa, OK
- Charlotte/Douglas International, Charlotte, NC
- Colorado Springs, Colorado Springs, CO

Program support will increase to accommodate the added projects. The TSA will increase Full Time Position staffing via the current hiring flexibilities available to agencies. Additional contract support personnel are also required to assist with site surveys/visits, airport outreach support, equipment testing and evaluation, and program management support.

TSA also will increase the procurement and deployment of Reduced Size EDSs by \$30 million to ETD-only airports to improve screening effectiveness and operational efficiencies.

Supporting Data

Estimated Number of Airports with Optimal Systems

Category	Total Number of TSA Airports	Entire Airport with Optimal Systems	Some Screening Areas with Optimal Systems	Total Number of Airports with at least one Optimal System	% of Airports with at least one Optimal System	Optimal Systems Inline Projects Funded FY 2009*	Optimal Systems Inline Projects Funded ARRA*
X	27	5	17	22	81%	2	9
I	55	15	17	32	58%	3	10
II	73	27	15	42	58%	6	5
III	122	21	3	24	20%	21	20
Total	277	68	52	120	43%	41	44

*FY 2009 and ARRA funds include Reduced Size EDS purchase for ETD-only airports.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

EBSP Expenditure Plan

Expenditure Plan: Appropriations, Obligations, and Expenditures

PROGRAM SPENDING PLAN: EBSP

APPROPRIATIONS IN \$ MILLIONS

Net Appropriated Funds ¹	1,232.85
Project Outlays End-of-Q1 FY09	108.01
Funds Obligated, Not Outlaid End-of-Q1 FY09	83.99
Unobligated Balance End-of-Q1 FY09	1,077.60

UNOBLIGATED BALANCES BY FY as of 30 JUNE 2009

FY09	Total
1,077.898	1,169.359

PLANNED OBLIGATIONS IN \$ MILLIONS AS OF 30 JUNE 2009

	Q1FY09	Q2FY09	Q3FY09	Q4FY09	Q1FY10	Q2FY10	Q3FY10	Q4FY10
Plan	18.727	70.074	388.865	838.877	145.768	-	-	-
Plan Cumulative	18.727	88.801	448.687	1,887.244	1,233.012	n/a	n/a	n/a
Cumulative % Allotment	10.30%	55.82%	24.08%	0.00%	0.89%			
Actual	1.929	39.183	88.855	-	-	-	-	-

PLANNED OUTLAYS IN \$ MILLIONS AS OF 30 JUNE 2009

	Q1FY09	Q2FY09	Q3FY09	Q4FY09	Q1FY10	Q2FY10	Q3FY10	Q4FY10
Plan	18.727	\$2.556	230.928	218.311	688.888	13.800	-	-
Plan Cumulative	18.727	71.283	322.208	538.619	1,219.186	1,232.986	n/a	n/a
Cumulative % Allotment	10.30%	23.30%	13.16%	0.00%	0.00%	0.90%	0.00%	0.00%
Actual	1.929	12.248	32.987	-	-	-	-	-

1. Total of all FY09 appropriations, actual and planned obligations, and actual and planned expenditures

EBSP Program Initiatives

Description of Initiative I – Program Operations and Management

- Description: The Program Operations and Management initiative is broken down into five sections.
 - 1. Operations and Compliance/Interim Solutions
 - Moves, Adds and Changes \$15.35 million
 - Equipment Warehousing \$3.5 million
 - 2. Program Support
 - Program, Resource and Data Management Services \$26.0 million
 - Testing Services \$234 million
 - Audits, Travel, Training and Certification \$1.2 million

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

- 3. Engineering Support
 - o Integration and Installation Management \$38.3 million
 - o Engineering Technical and Design Support \$13.6 million
- 4. TSA Systems Integration Facility (TSIF) Support \$4.8 million
- 5. TSIF Building Purchase \$7.4 million
- 6. PC&B \$18.8 million
- Projected FY 2009 Obligations and Expenditures: \$97.5 million
- Projected ARRA Obligations and Expenditures: \$54.85 million

Description of Initiative II – LOI (FY 2009)

- Previously committed multiyear agreements for facility modifications
- Projected FY 2009 Obligations and Expenditures: \$200.0 million

Description of Initiative III – EDS

- FY 2009
 - o The following EDSs will be purchased and installed:
 - Equipment for new terminals to permit TSA to screen bags on opening day to ensure that the airports do not rely on other screening solutions
 - Equipment necessary to maintain 100 percent screening compliance at existing installations
 - Equipment to fulfill existing TSA facility modification agreements (for example, EDS machines for LOI or Other Transactional Agreement (OTA) airports) for optimal in-line screening solutions that remove lobby congestion and decrease security concerns
 - Equipment to airports that have not received facility modifications funding but are proceeding with optimal system projects via their own financing, which are the most cost effective
 - o Projected FY 2009 Obligations and Expenditures: \$146.6 million
 - o Activities and Milestones: Installs based on airport schedules
- ARRA
 - o Recapitalization efforts for airports with EDS solutions at the end of their life cycle
 - o ETD-only airports that now require EDS technology to meet the screening requirements to improve screening effectiveness and to improve operational efficiencies through improved throughput and reduced on-the-job injuries
 - o Projected ARRA Obligations and Expenditures: \$94.2 million
 - o Activities and Milestones: Purchases to occur in Q3 FY 2009; installs based on airport schedules.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Description of Initiative IV – New Facility Modification Agreements to Construct a Checked Baggage Inspection System (CBIS).

- FY 2009 – OTAs will be used to fund facility modifications to construct a CBIS at eight airports.
 - See Appendix M for Obligation data.
 - See Appendix O for Milestones.
 - Projected FY 2009 Obligations and Expenditures: \$67.32 million
- ARRA – OTAs will be used to fund facility modifications to construct a CBIS at 25 airports. TSA will assess the ability to add projects after completion of the cost validation for these 25 airports, which provides the anticipated cost difference between airport request funds and TSA-awarded funds.
 - See Appendix N for Obligation data.
 - See Appendix P for Milestones.
 - Projected ARRA Obligations and Expenditures: \$499.2 million

Description of Initiative V – Technology/Engineering Initiatives

- FY 2009 – Contracting Officer's Technical Representative/Engineering Initiatives will address:
 - Design and configuration changes/modifications (includes reconfiguration).
 - Requirements and Engineering Change Proposals.
 - Change in government guidance/objectives to improve efficiencies and equipment performance, such as employing equipment upgrades across the entire fleet of EDS (example: performance upgrade all CT-80 to CT-80DR) and implementing local networking at sites with multiple CT-80/CT-80DR systems to improve data collection efficiencies.
 - Non-operational issues, such as problems with repairs associated with equipment redeployment and out-of warranty.
 - Lack of commonality among checked baggage screening solutions.
 - Limitations on deployment of screening solutions based on existing site conditions.
 - Variances in technology capabilities that limit TSA flexibility in providing optimal screening solutions.
 - Projected Obligations and Expenditures: Total FY09 Engineering Initiatives: \$17.6 million
- ASP will address:
 - Remote visibility into the baggage resolution and screening areas in case of emergency to aid in threat identification and response.
 - A means to create an overall situational awareness to support oversight control for loss prevention, remote supervision, training, staffing, performance evaluation and legal or investigative needs with recordation.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

- An additional layer of security for the locations where TSA screens checked baggage to reduce the risk of threats from being introduced into checked baggage.
- Projected Obligations and Expenditures: Total FY 2009 ASP Initiatives: \$5.0 million
- Projected Obligations and Expenditures: Total ARRA ASP Initiatives: \$40.6 million
- Security Technology Integrated Program (STIP) will address:
 - Equipment in-service upgrades and automated data retrieval on equipment and screener performance to increase equipment availability, reliability and effectiveness; improve performance management and reduce overall operating and support costs.
 - Equipment replacement, reconfiguration and deployment strategies to increase throughput, systems capacity and effectiveness.
 - Projected Obligations and Expenditures: Total FY 2009 STIP Initiatives: \$8.0 million
- OI will address:
 - System integration and equipment purchases required for operational test and evaluation activities.
 - Projected Obligations and Expenditures: Total FY 2009 OI Initiatives: \$2.0 million
- Projected Obligations and Expenditures: Total FY 2009 Technology/Engineering Initiatives: \$32.6 millions
- Projected Obligations and Expenditures: Total ARRA Technology/Engineering Initiatives: \$40.6 millions

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

IV. Appendices

Appendix A. Abbreviations/Acronyms

ARRA	American Recovery and Reinvestment Act of 2009
AIT	Advanced Imaging Technology
ASP	Advanced Surveillance Program
AT	Advanced Technology
ATSA	Aviation & Transportation Security Act
BAO	Bomb Appraisal Officer
BLS	Bottled Liquids Scanner
CAD	Chemical Analyzer Detector
CAT/BPSS	Credential Authentication Technology/Boarding Pass Scanning Systems
CBIS	Checked Baggage Inspection System
DHS	Department of Homeland Security
EBSP	Electronic Baggage Screening Program
EDS	Explosives Detection Systems
EMD	Enhanced Metal Detector
ETD	Explosives Trace Detection
FAA	Federal Aviation Administration
FOC	Full Operational Capability
FY	Fiscal Year
HSA	Homeland Security Act of 2002
IOC	Initial Operational Capability
LOI	Letter of Intent
Next Gen ETD	Next Generation Explosives Trace Detector
OI	Operational Integration
OT&E	Operational Testing and Evaluation
OTA	Other Transactional Agreement
PC&B	Personnel Compensation and Benefits
PPA	Program, Project and Activity
PSP	Passenger Screening Program
QT&E	Qualification Testing and Evaluation
STIP	Security Technology Integration Program

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix A. Abbreviations/Acronyms (continued)

TIP	Threat Image Projection
TRX	Threat Image Projection (TIP) Ready X-Ray
TSA	Transportation Security Administration
TSIF	TSA Systems Integration Facility
TSO	Transportation Security Officer
UCS	Universal Conveyor Systems

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix B. Airport Codes

Airport Code	Airport Name	Airport Location
ACK	Nantucket Memorial	Nantucket, MA
AMA	Rick Husband Amarillo International	Amarillo, TX
ASE	Aspen-Pitkin County/Sardy Field	Aspen, CO
ATL	Hartsfield - Jackson Atlanta International	Atlanta, GA
BOI	Boise Air Terminal/Gowen Field	Boise, ID
BZN	Gallatin Field	Bozeman, MT
CHA	Lovell Field	Chattanooga, TN
CHS	Charleston AFB/International	Charleston, SC
CLT	Charlotte/Douglas International	Charlotte, NC
CMH	Port Columbus International	Columbus, OH
CMI	University of Illinois - Willard	Savoy, IL
COD	Yellowstone Regional	Cody, WY
COS	Colorado Springs	Colorado Springs, CO
CVG	Cincinnati/Northern Kentucky International	Covington, KY
DAY	James M Cox Dayton International	Dayton, OH
DCA	Ronald Reagan Washington National	Washington, DC
EGE	Eagle County Regional	Eagle, CO
EWK	Newark Liberty International	Newark, NJ
FAT	Fresno Yosemite International	Fresno, CA
GEG	Spokane International	Spokane, WA
GPI	Glacier Park International	Kalispell, MT
GRR	Gerald R. Ford International	Grand Rapids, MI
GUC	Gunnison-Crested Butte Regional	Gunnison, CO
HDN	Yampa Valley	Hayden, CO
HLN	Helena Regional	Helena, MT
HNL	Honolulu International	Honolulu, HI
HOU	William P. Hobby	Houston, TX
HSV	Huntsville International - Carl T Jones Field	Huntsville, AL
IAD	Washington Dulles International	Washington, DC
IAH	George Bush Intercontinental/Houston	Houston, TX

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY**Appendix B. Airport Codes (continued)**

Airport Code	Airport Name	Airport Location
ICT	Wichita Mid-Continent	Wichita, KS
ITO	Hilo International	Hilo, HI
JAC	Jackson Hole	Jackson Hole, WY
JFK	John F. Kennedy International	New York, NY
LGA	La Guardia	New York, NY
LIT	Little Rock National	Little Rock, AR
LSE	La Crosse Municipal	La Crosse, WI
MCO	Orlando International	Orlando, FL
MFR	Rogue Valley International -- Medford	Medford, OR
MIA	Miami International	Miami, FL
MKK	Molokai Airport	Kaunakakai, HI
MSP	Minneapolis -- St. Paul International/Wold-Chamberlain	Minneapolis, MN
MSY	Louis Armstrong New Orleans International	New Orleans, LA
OAK	Metropolitan Oakland International	Oakland, CA
OGG	Kahului	Maui, HI
ORD	Chicago O'Hare International	Chicago, IL
PFN	Panama City-Bay County International	Panama City, FL
PHL	Philadelphia International	Philadelphia, PA
PHX	Phoenix Sky Harbor International Airport	Phoenix, AZ
PIE	St. Petersburg-Clearwater International	St. Petersburg, FL
PIT	Pittsburgh International	Pittsburgh, PA
PNS	Pensacola Regional	Pensacola, FL
PWM	Portland International Jetport	Portland, ME
RDM	Roberts Field	Redmond, OR
RDU	Raleigh-Durham International	Raleigh, NC
RNO	Reno/Tahoe International	Reno, NV
ROC	Greater Rochester International	Rochester, NY
SAN	San Diego International	San Diego, CA
SAT	San Antonio International	San Antonio, TX

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix B. Airport Codes (continued)

Airport Code	Airport Name	Airport Location
SBA	Santa Barbara Municipal	Santa Barbara, CA
SFO	San Francisco International	San Francisco, CA
SJC	Norman Y. Mineta San Jose International	San Jose, CA
SMF	Sacramento International	Sacramento, CA
SMX	Santa Maria Public Airport	Santa Maria, CA
SNA	John Wayne Airport-Orange County	Orange County, CA
STL	Lambert-Saint Louis International	St. Louis, MO
SUN	Friedman Memorial	Hailey, ID
TLH	Tallahassee Regional	Tallahassee, FL
TRI	Tri-Cities Regional	Bristol/Johnson/Kingsport, TN
TUL	Tulsa International	Tulsa, OK
TUS	Tucson International	Tucson, AZ
UTA	Tunica Municipal	Tunica, MS

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix C. Passenger Screening Program (PSP) Deployments by Airport

The number of procurements may not equal the number of deployments in one fiscal year. Planned airports are a function of the quantity and timing of units procured previously and the quantity of deployments being achieved. The chart below accounts for all deployments scheduled to occur by September 30, 2009.

Airport	Size	Planned ETD	Actual ETD	Planned AT	Actual AT	Planned AIT	Actual AIT	Planned SLS	Actual SLS	Planned CAT	Actual CAT	Planned Tech Cost	Actual Tech Cost	Planned Set Up Cost	Actual Set Up Cost
JFK	X	22		10	29			23		35		\$ 4,220,000	\$ 1,902,110	\$ 572,089	\$ 874,582
LAX	X	14			9			29				\$ 1,827,500	\$ 196,770	\$ 119,257	\$ 90,474
DCA	X	3					2	5				\$ 405,000	\$ 308,394	\$ 25,088	\$ 90,542
BWI	X	8			1			8		14		\$ 1,095,000	\$ 172,238	\$ 102,364	\$ 30,158
IAD	X	4			9			9				\$ 577,500	\$ 1,033,428	\$ 35,587	\$ 180,848
ORD	X	13		51	51	2		19				\$ 8,189,500	\$ 3,345,090	\$ 1,722,527	\$ 1,538,055
MIA	X	6			13			10				\$ 735,000	\$ 2,239,094	\$ 45,890	\$ 302,054
LGA	X	3		9	9			9				\$ 1,642,500	\$ 1,550,142	\$ 302,919	\$ 271,422
EWK	X	15		12	1	3		12				\$ 3,333,000	\$ 65,590	\$ 584,855	\$ 30,158
IAH	X	12		11	11			11				\$ 2,507,500	\$ 721,490	\$ 404,401	\$ 331,738
BOS	X	9		16	13	9		16				\$ 4,105,000	\$ 2,239,094	\$ 825,482	\$ 392,054
PHL	X	2		14	21			9				\$ 2,207,500	\$ 1,377,390	\$ 448,909	\$ 633,318
DTW	X	19		34	18			12				\$ 5,640,000	\$ 3,100,284	\$ 1,126,858	\$ 542,944
DFW	X	13			8			22				\$ 1,605,000	\$ 1,377,904	\$ 100,226	\$ 241,254
ATL	X	15			18		3	11				\$ 1,312,500	\$ 1,643,211	\$ 84,063	\$ 676,607
SFO	X	12		14	10		1	14				\$ 2,995,000	\$ 1,876,577	\$ 501,274	\$ 346,901
MSP	X	9		10	10			10				\$ 2,165,000	\$ 655,900	\$ 359,810	\$ 301,580
MCO	X	3		10	9			10				\$ 1,805,000	\$ 1,550,142	\$ 335,210	\$ 271,422
MNL	X	9		9	8			8				\$ 2,002,500	\$ 1,550,142	\$ 327,519	\$ 271,422
DEN	X	4						7				\$ 592,500	\$ -	\$ 31,331	\$ -
SJU	X	6		6	4			6				\$ 1,455,000	\$ 262,380	\$ 226,546	\$ 120,632
LAS	X	1						12				\$ 510,000	\$ -	\$ 29,696	\$ -
SEA	X	7		9	10			9				\$ 1,882,500	\$ 655,900	\$ 319,319	\$ 301,580
CLT	X	3		5	4			5				\$ 992,500	\$ 262,360	\$ 173,755	\$ 120,632
SAN	I	4		8	7			8				\$ 1,540,000	\$ 459,130	\$ 274,728	\$ 211,108
PHX	X	7			1			11				\$ 832,500	\$ 65,590	\$ 52,163	\$ 30,158
FLL	X	13		9	6			9				\$ 2,342,500	\$ 590,310	\$ 343,919	\$ 271,422
GLM	I			5				1				\$ 662,500	\$ -	\$ 152,923	\$ -
CVG	X	4		5	4			5				\$ 1,090,000	\$ 588,952	\$ 179,988	\$ 120,632
IND	I	1		8	5			5				\$ 572,500	\$ 327,950	\$ 165,555	\$ 150,790

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix C. PSP Deployments by Airport (continued)

Airport	SEZE	Planned ETD	Actual ETD	Planned AT	Actual AT	Planned AJT	Actual AJT	Planned BL\$	Actual BL\$	Planned CAT	Actual CAT
PDX	I	3		6	5			6			
MEM	I	4		4				5			
STL	X	3		6	5			5			
JAX	I	4		2	2		1	2			
ANC	I			3	3			3			
SYR	II			3				3			
SJC	I	2		6	2			6			
SLC	I			6	5		1	6			
BUF	I			2	3			2			
SNA	I	5		4				4			
SAT	I	4		3	3			3			
PIT	I			4	4			4			
IND	IV				1			5			
GSN	II			2	3			1			
TPA	I	1		7	6		2	7			
PBI	I	1		4				4			
ONT	I	1		2				2			
MKE	I	2		4	4			4			
MDW	I			5	5						
MCI	I	1		10	11						
HOU	I			6							
DAL	I	1		2	3						
CLE	I	4		5	4						
BUR	I	1		2	2						
BHM	I			2							
BCL	I			3	3						
TUS	I	1		6	2						
SNA	I	1		4	4						
SFB	II	1		3	2						
PVD	I	2		2	2						

Planned Tech Cost	Actual Tech Cost	Planned Set Up Cost	Actual Set Up Cost
\$ 1,155,000	\$ 881,190	\$ 206,046	\$ 150,790
\$ 927,900	\$ -	\$ 147,697	\$ -
\$ 1,165,000	\$ 327,950	\$ 206,046	\$ 150,790
\$ 565,000	\$ 488,673	\$ 80,882	\$ 105,637
\$ 487,500	\$ 196,770	\$ 96,873	\$ 80,474
\$ 487,500	\$ -	\$ 96,873	\$ -
\$ 1,095,800	\$ 344,476	\$ 201,948	\$ 60,316
\$ 875,000	\$ 1,315,307	\$ 193,748	\$ 196,111
\$ 325,000	\$ 516,714	\$ 64,582	\$ 90,474
\$ 850,000	\$ -	\$ 149,664	\$ -
\$ 727,500	\$ 196,770	\$ 113,278	\$ 90,474
\$ 650,000	\$ 282,380	\$ 128,164	\$ 120,632
\$ 187,500	\$ 85,580	\$ 10,685	\$ 30,158
\$ 287,500	\$ 196,770	\$ 62,449	\$ 90,474
\$ 1,197,500	\$ 1,341,622	\$ 230,137	\$ 271,590
\$ 710,000	\$ -	\$ 133,284	\$ -
\$ 385,000	\$ -	\$ 66,682	\$ -
\$ 770,000	\$ 688,662	\$ 137,364	\$ 120,632
\$ 625,000	\$ 881,190	\$ 150,790	\$ 150,790
\$ 1,310,000	\$ 1,884,618	\$ 305,680	\$ 331,736
\$ 750,000	\$ -	\$ 180,848	\$ -
\$ 310,000	\$ 516,714	\$ 64,416	\$ 90,474
\$ 865,000	\$ 688,662	\$ 167,190	\$ 120,632
\$ 310,000	\$ 344,476	\$ 64,416	\$ 60,316
\$ 250,000	\$ -	\$ 60,316	\$ -
\$ 375,000	\$ 516,714	\$ 90,474	\$ 60,474
\$ 810,000	\$ 131,160	\$ 185,048	\$ 60,316
\$ 560,000	\$ 282,380	\$ 124,732	\$ 120,632
\$ 435,000	\$ 344,476	\$ 96,574	\$ 60,316
\$ 370,000	\$ 344,476	\$ 68,516	\$ 60,316

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix C. PSP Deployments by Airport (continued)

Airport	SIZE	Planned ETD	Actual ETD	Planned AT	Actual AT	Planned AIT	Actual AIT	Planned BLB	Actual BLB	Planned CAT	Actual CAT	Planned Tech Cost	Actual Tech Cost	Planned Set Up Cost	Actual Set Up Cost
ORF	I	1		2	2							\$ 310,000	\$ 344,476	\$ 64,416	\$ 60,316
MSY	I	1		4								\$ 560,000	\$ -	\$ 124,732	\$ -
GEG	I			2	2							\$ 250,000	\$ 344,476	\$ 60,316	\$ 60,316
DAY	I			6								\$ 760,000	\$ -	\$ 180,948	\$ -
ROC	II			6	2							\$ 750,000	\$ 344,476	\$ 180,948	\$ 60,316
SMF	I	1		8	5							\$ 1,185,000	\$ 881,180	\$ 275,522	\$ 150,790
RSW	I	1		4								\$ 560,000	\$ -	\$ 124,732	\$ -
RNO	I	2		2	1							\$ 370,000	\$ 172,238	\$ 66,516	\$ 30,158
OMA	I			2	2							\$ 250,000	\$ 344,476	\$ 60,316	\$ 60,316
OKC	I			2	2							\$ 250,000	\$ 344,476	\$ 60,316	\$ 60,316
GGG	I	2		5	2							\$ 870,000	\$ 131,180	\$ 188,148	\$ 60,316
OAK	I			4	4							\$ 500,000	\$ 588,852	\$ 120,632	\$ 120,632
AUS	I	2		4	2							\$ 620,000	\$ 131,180	\$ 128,532	\$ 60,316
CMH	I	1		3								\$ 435,000	\$ -	\$ 94,574	\$ -
STT	II	1		6	6							\$ 810,000	\$ 383,540	\$ 185,048	\$ 180,948
MHT	I	1		3	3							\$ 435,000	\$ 516,714	\$ 94,574	\$ 60,474
MDT	II	1		3								\$ 435,000	\$ -	\$ 94,574	\$ -
LH	I	2		3	4							\$ 495,000	\$ 262,360	\$ 94,574	\$ 120,632
LGB	I			2	4							\$ 250,000	\$ 262,360	\$ 60,316	\$ 120,632
FAI	II			2	2							\$ 250,000	\$ 131,180	\$ 60,316	\$ 60,316
STX	III	1		3	3							\$ 435,000	\$ 198,770	\$ 94,574	\$ 90,474
PPG	III	4		1	1							\$ 365,000	\$ 65,590	\$ 48,558	\$ 30,158
FAT	II			2	2							\$ 250,000	\$ 131,180	\$ 60,316	\$ 60,316
KOA	I	1		3	4							\$ 435,000	\$ 262,360	\$ 94,574	\$ 120,632
GRR	II			4	2							\$ 500,000	\$ 344,476	\$ 120,632	\$ 60,316
MLB	II			2								\$ 250,000	\$ -	\$ 60,316	\$ -
DAB	II			2								\$ 250,000	\$ -	\$ 60,316	\$ -
HPN	II			2								\$ 250,000	\$ -	\$ 60,316	\$ -
ABE	II			2	2							\$ 250,000	\$ 131,180	\$ 60,316	\$ 60,316
RIC	I	1		6	2		1					\$ 810,000	\$ 285,377	\$ 185,048	\$ 105,637

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix C. PSP Deployments by Airport (continued)

Airport	SIZE	Planned ETD	Actual ETD	Planned AT	Actual AT	Planned AIT	Actual AIT	Planned BLS	Actual BLS	Planned CAT	Actual CAT	Planned Tech Cost	Actual Tech Cost	Planned Set Up Cost	Actual Set Up Cost
ABO	I	2										\$ 120,000	\$ -	\$ 8,200	\$ -
ABI	II	1										\$ 80,000	\$ -	\$ 4,100	\$ -
AMA	II	1										\$ 60,000	\$ -	\$ 4,100	\$ -
BLI	II	2										\$ 120,000	\$ -	\$ 8,200	\$ -
BMI	II	3										\$ 180,000	\$ -	\$ 12,300	\$ -
BTX	II	1										\$ 80,000	\$ -	\$ 4,100	\$ -
CEF	II	1										\$ 60,000	\$ -	\$ 4,100	\$ -
CHO	II	1										\$ 80,000	\$ -	\$ 4,100	\$ -
DID	II	1										\$ 60,000	\$ -	\$ 4,100	\$ -
ELF	I	3										\$ 180,000	\$ -	\$ 12,300	\$ -
ERI	II	1										\$ 60,000	\$ -	\$ 4,100	\$ -
GSO	I	1										\$ 80,000	\$ -	\$ 4,100	\$ -
GBP	II	1										\$ 60,000	\$ -	\$ 4,100	\$ -
ILM	II	1										\$ 80,000	\$ -	\$ 4,100	\$ -
ITC	II	1										\$ 60,000	\$ -	\$ 4,100	\$ -
JWA	III	1										\$ 60,000	\$ -	\$ 4,100	\$ -
LEX	II	2										\$ 120,000	\$ -	\$ 8,200	\$ -
LNK	II	1										\$ 80,000	\$ -	\$ 4,100	\$ -
MBS	II	1										\$ 60,000	\$ -	\$ 4,100	\$ -
MGM	II	1										\$ 60,000	\$ -	\$ 4,100	\$ -
MYR	II	1										\$ 60,000	\$ -	\$ 4,100	\$ -
PIE	II	1										\$ 60,000	\$ -	\$ 4,100	\$ -
PNS	II	1										\$ 80,000	\$ -	\$ 4,100	\$ -
PSE	III	2										\$ 120,000	\$ -	\$ 8,200	\$ -
SEB	II	1										\$ 80,000	\$ -	\$ 4,100	\$ -
SPS	III	1										\$ 60,000	\$ -	\$ 4,100	\$ -
VLD	III	1										\$ 60,000	\$ -	\$ 4,100	\$ -
UNV	IV	2										\$ 120,000	\$ -	\$ 8,200	\$ -
BPT	IV	1										\$ 60,000	\$ -	\$ 4,100	\$ -
TUL	IV	N/A		N/A		N/A	1	N/A		N/A		\$ -	\$ 154,197	\$ -	\$ 45,321
TOTAL		346	0	472	427	11	12	401	0	48	0	\$ 97,671,000	\$ 48,480,528	\$ 17,180,780	\$ 13,421,318

*TUL was included as a new airport in the first quarter and second quarter expenditure plans. The "N/A" identified it as new airport, which meant there was no initial plan to compare the actual plan to.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix D. PSP FY 2009 Summary Spend Plan

Technology	Initial # of Units	Revised # of Units	Approved FY09 Funds	Revised FY09 Funds
Advanced Technology *	436	488	\$54.50	\$61.00
Universal Conveyor Systems	200	0	\$25.00	\$0.00
Advanced Imaging Technology	175	175	\$28.90	\$28.90
Credential Authentication Technology *	288	0	\$6.50	\$0.00
Bottled Liquids Scanners *	200	600	\$7.50	\$22.70
Explosives Trace Detectors	100	0	\$6.00	\$0.50
Subtotal			\$128.40	\$113.10
* Equipment quantities to be purchased with Fiscal Year 2009 funds and carryover funds were reallocated for Advanced Technology, Bottled Liquids Scanners, and Credential Authentication Technology.				
Program Operations and Management				
Integration			\$30.55	\$31.90
Warehouse			\$1.25	\$5.30
Engineering Support			\$4.10	\$7.70
Testing (IV&V)			\$3.30	\$0.05
Data Collection			\$3.00	\$0.00
TSA Systems Integration Facility (TSIF) Support			\$1.50	\$5.90
TSA Systems Integration Facility (TSIF) building purchase			\$0.00	\$2.40
Program and Data Management			\$12.20	\$9.30
Travel, Training, Supplies			\$1.10	\$0.95
Subtotal			\$57.00	\$63.50

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix D. PSP FY 2009 Summary Spend Plan (continued)

	Approved FY09 Funds	Revised FY09 Funds
Technical and Engineering Initiatives		
Security Technology Integration Program	\$7.60	\$10.50
Operational Integration of Emerging Technology	\$7.00	\$10.00
Threat Image Projection	\$4.00	\$4.00
Engineering Changes	\$2.40	\$0.50
Exit Lanes Data Collection	\$1.60	\$1.60
Subtotal	\$22.60	\$26.60
Safety and Optimization		
Equipment	\$5.00	\$5.00
System Integrator	\$3.00	\$3.00
Engineering Support	\$2.50	\$2.50
Airport Projects	\$2.00	\$2.00
Project Logistics	\$1.00	\$1.00
Subtotal	\$13.50	\$13.50
Checkpoint Reconfiguration		
Ancillary Equipment	\$3.00	\$3.00
Glass Partitions	\$2.70	\$2.70
Checkpoint Optimizations	\$1.70	\$1.70
Divest/Compos ure/Roller Tables	\$1.50	\$1.50
Project Logistics	\$1.50	\$1.50
Engineering and Technical Support	\$1.00	\$1.00
Travel	\$0.10	\$0.10
Subtotal	\$11.50	\$11.50

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix D. PSP FY 2009 Summary Spend Plan (continued)

Advanced Surveillance Program	Approved FY09 Funds	Revised FY09 Funds
Boston (BOS)	\$4.30	\$1.80
Orlando (MCO)	\$3.30	\$0.00
Philadelphia (PHL)	\$1.60	\$3.40
Phoenix (PHX)	\$0.00	\$0.00
Atlanta (ATL)	\$0.00	\$0.00
Chicago (ORD)	\$0.80	\$0.80
Cleveland (CLE)	\$0.10	\$0.10
Louis Munoz Marin (SJU)	\$0.10	\$0.10
Long Beach (LGB)	N/A	\$0.30
Providence (PVD)	N/A	\$1.30
San Francisco	N/A	\$2.40
Program Support	\$0.80	\$0.80
Subtotal	\$11.00	\$11.00
Personnel Compensation and Benefits	\$6.00	\$6.00
Total*	\$250.00	\$245.20

*\$4.8 million was reallocated from the checkpoint support Program, Project and Activity.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix E. PSP American Recovery and Reinvestment Act (ARRA) Summary Spend Plan

Technology	Initial # of Units	Revised # of Units	Approved ARRA Funds	Revised ARRA Funds
Advanced Technology *	755	611	\$94.40	\$76.40
Universal Conveyor Systems	275	228	\$34.40	\$28.50
Advanced Imaging Technology	200	200	\$32.20	\$32.20
Credential Authentication Technology	0	800	\$0.00	\$18.00
Bottled Liquids Scanners	500	500	\$18.80	\$18.80
Explosives Trace Detectors	300	400	\$18.00	\$22.00
Chemical Analyzer Detectors	N/A	140	N/A	\$7.00
Subtotal			\$197.80	\$202.90
* Reduced to add Credential Authentication Technology to ARRA spend plan.				
Program Operations and Management				
Integration			\$57.90	\$68.20
Testing (IV&V)			\$2.00	\$2.00
Program and Data Management			\$23.00	\$7.50
Subtotal			\$82.90	\$77.70
Technical and Engineering Initiatives				
Engineering Changes			\$9.90	\$9.90
Subtotal			\$9.90	\$9.90

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix E. PSP ARRA Summary Spend Plan (continued)

Advanced Surveillance Program	Approved ARRA Funds	Revised ARRA Funds
Ronald Reagan Washington National	\$0.60	\$1.90
Cincinnati/Northern Kentucky International	\$1.80	\$0.70
Spokane International	\$1.10	\$1.70
Metropolitan Oakland International	\$2.20	\$0.00
Boise Gowen Field Air Terminal	N/A	\$0.80
Kent County Airport	N/A	\$0.60
Washington Dulles International	N/A	\$2.60
Will Rogers World	N/A	\$0.70
Chicago Midway International	N/A	\$1.40
Eppler Airfield	N/A	\$0.70
James M. Cox Dayton International Airport	N/A	\$0.45
Kansas City International	N/A	\$2.80
Adams Field	N/A	\$0.40
Tampa International	N/A	\$2.10
Subtotal	\$5.70	\$16.85
Personnel Compensation and Benefits	\$3.80	\$3.80
Total*	\$300.00	\$311.15

Numbers may not add due to rounding.

*Revised ARRA funds: \$11.1 million was shifted from Explosives Detection Systems to PSP for Advanced Surveillance Program/Closed Circuit Television projects.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix F. PSP FY 2009 Obligation Data

Spend Plan Categories	\$ in millions	Planned Obligation Date	\$ in millions	Revised Obligation Date
Advanced Technology	\$54.50	Jul-09	\$61.00	Nov-09
Universal Conveyor Systems	\$25.00	Aug-09	\$0.00	Mar-10
Advanced Imaging Technology	\$28.90	Jul-09	\$28.90	Dec-09
Credential Authentication Technology	\$6.50	Jul-09	\$0.00	Sep-09
Bottled Liquids Scanners	\$7.50	Jul-09	\$22.70	Sep-09
Explosives Trace Detectors	\$6.00	Jul-09	\$0.50	Sep-09
Integration	\$30.55	Jul-09	\$31.90	Sep-09
Program Operations and Management	\$26.45	Ongoing	\$31.60	Ongoing
Technical and Engineering Initiatives	\$22.60	Ongoing	\$26.60	Ongoing
Safety and Optimization	\$13.50	Ongoing	\$13.50	Ongoing
Checkpoint Reconfiguration	\$11.50	Ongoing	\$11.50	Ongoing
Advanced Surveillance Program	\$11.00	Ongoing	\$11.00	Ongoing
Personnel Compensation and Benefits	\$6.00	Ongoing	\$6.00	Ongoing
Subtotal	\$250.00		\$245.20	

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix G. PSP ARRA Obligation Data

Spend Plan Categories	\$ in millions	Planned Obligation Date	\$ in millions	Revised Obligation Date
Advanced Technology	\$94.40	Jul-09	\$76.40	May-09 Nov-09
Universal Conveyor Systems	\$34.40	Aug-09	\$28.50	Mar-10
Advanced Imaging Technology	\$32.20	Jul-09	\$32.20	Sep-09
Credential Authentication Technology	\$0.00	N/A	\$18.00	Sep-09
Bottled Liquids Scanners	\$18.80	Jul-09	\$18.80	Sep-09
Explosives Trace Detectors	\$18.00	Jul-09	\$22.00	Sep-09
Chemical Analyzer Detectors	N/A	N/A	\$7.00	Sep-09 Dec-09
Integration	\$57.90	Jul-09	\$68.20	Sep-09
Program Operations and Management	\$25.00	Ongoing	\$9.50	Ongoing
Technical and Engineering Initiatives	\$9.90	Ongoing	\$9.90	Ongoing
Advanced Surveillance Program	\$5.70	Ongoing	\$16.85	Ongoing
Personnel Compensation and Benefits	\$3.80	Ongoing	\$3.80	Ongoing
Subtotal	\$300.00		\$311.15	

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix H. PSP FY 2009 Milestones

Advanced Technology	Planned	Revised
Initial Qualified Data Package Down Select	Mar-09	Mar-09
Qualification Testing and Evaluation (QT&E) Begins	Mar-09	Aug-09
Operational Testing and Evaluation (OT&E) Begins	Apr-09	Aug-09
Contract Award	Jul-09	Nov-09
Advanced Imaging Technology		
QT&E Begins	Feb-09	Aug-09
OT&E Begins	Apr-09	Aug-09
Request for Proposals Released	Jun-09	Jun-09
Contract Award	Jul-09	Sep-09
Bottled Liquids Scanners		
QT&E Begins	Mar-09	Jun-09
OT&E Begins	Mar-09	Jul-09
Contract Award	Jul-09	Sep-09
Advanced Surveillance Program		
Boston Logan International	May-09	Sep-09
Philadelphia International	May-09	Sep-09
Orlando International	May-09	N/A
Phoenix Sky Harbor International	May-09	N/A
Chicago O'Hare International	N/A	Sep-09
Cleveland Hopkins International	N/A	Sep-09
Luis Munoz Marin International	N/A	Sep-09
Long Beach	N/A	Sep-09
Theodore Francis Green International	N/A	Sep-09
San Francisco International	N/A	Sep-09

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix I. PSP ARRA Milestones

Advanced Technology	Planned	Revised
Initial Qualified Data Package Down Select	Mar-09	Mar-09
Qualification Testing and Evaluation (QT&E) Begins	Mar-09	Aug-09
Operational Testing and Evaluation (OT&E) Begins	Apr-09	Aug-09
Contract Award	Jul-09	Nov-09
Universal Conveyor System		
QT&E Begins	TBD	TBD
OT&E Begins	TBD	TBD
Contract Award	TBD	Mar-10
Advanced Imaging Technology		
QT&E Begins	Feb-09	Aug-09
OT&E Begins	Apr-09	Aug-09
Request for Proposals Released	Jun-09	Jun-09
Contract Award	Jul-09	Sep-09
Credential Authentication Technology		
QT&E Begins	Aug-09	Aug-09
OT&E Begins	Aug-09	Aug-09
Contract Award	Sep-09	Sep-09
Bottled Liquids Scanners		
QT&E Begins	Mar-09	Jun-09
OT&E Begins	Mar-09	Jul-09
Contract Award	Jul-09	Sep-09
Next Gen Explosives Trace Detectors		
QT&E Began	Nov-07	Nov-07
OT&E Began	Mar-08	Mar-08
Contract Award	Aug-08	Aug-08

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix I. PSP ARRA Milestones (continued)

Advanced Surveillance Program	Planned	Revised
Ronald Reagan Washington National	Jun-09	Jun-09
Cincinnati/Northern Kentucky International	Jun-09	Jun-09
Spokane International	Jun-09	Jul-09
Metropolitan Oakland International	Jun-09	N/A
Boise Gowen Field Air Terminal	N/A	Jul-09
Kent County Airport	N/A	Jul-09
Washington Dulles International	N/A	Sep-09
Will Rogers World	N/A	Sep-09
Chicago Midway International	N/A	Sep-09
Eppley Airfield	N/A	Sep-09
James M Cox Dayton International	N/A	Sep-09
Kansas City International	N/A	Sep-09
Adams Field	N/A	Sep-09
Tampa International	N/A	Sep-09

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix J. PSP FY 2009 Actual vs. Anticipated Unobligated Balance, as of June 30, 2009

FY09				Anticipated
Spend Plan Category (\$M)	Budgeted	Obligated	Unobligated	Unobligated at end of FY09
Checkpoint Technology	\$203.20	\$22.90	\$180.30	\$90.00
Checkpoint Reconfiguration	\$11.50	\$5.10	\$6.40	\$0.00
ASP	\$11.00	\$0.00	\$11.00	\$0.00
Safety Optimization	\$13.50	\$0.00	\$13.50	\$3.70
PC&B	\$6.00	\$3.80	\$2.20	\$1.15
Total	\$245.20	\$31.80	\$213.40	\$94.85

FOR OFFICIAL USE ONLY

WARNING: This document is **FOR OFFICIAL USE ONLY (FOUO)**. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix K. PSP ARRA Actual vs. Anticipated Unobligated Balance, as of June 30, 2009

ARRA Spend Plan Category (\$M)	Budgeted	Obligated	Unobligated	Anticipated Unobligated at end of FY09
Checkpoint Technology	\$290.50	\$2.90	\$287.60	\$138.30
Advanced Surveillance Program	\$16.85	\$2.50	\$14.35	\$0.00
Personnel Compensation and Benefits	\$3.80	\$0.00	\$3.80	\$3.80
Total	\$311.15	\$5.40	\$305.75	\$142.10

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix L. Electronic Baggage Screening Program (EBSP) FY 2009 Obligation by Project

Project	Spend Plan	Project Timelines				Project Cost		Obligation Schedule		Obligation Balances			Expenditures
		Ant. Start Date	Actual Start Date	Ant. End Date	Actual End Date	Initial Dollar Amt.	Revised Dollar Amt.	Planned Obligation	Actual Obligation	Obligated	Unobligated Balance	Anticipated Unobligated	
JFK	LOI	Sep-08	Sep-08	Sep-13	-	\$78.00	-	May-09	-	\$0.00	\$78.00	\$0.00	\$0.00
ENR	LOI	Sep-08	Sep-08	Sep-13	-	\$60.00	-	May-09	-	\$0.00	\$60.00	\$0.00	\$0.00
LGA	LOI	Sep-08	Sep-08	Sep-13	-	\$62.00	-	May-09	-	\$0.00	\$62.00	\$0.00	\$0.00
ORD	OTA	Aug-09	-	Feb-10	-	\$19.80	-	May-09	-	\$0.00	\$19.80	\$0.00	\$0.00
ICT	OTA	Dec-09	-	Mar-11	-	\$8.25	-	Sep-09	-	\$0.00	\$8.25	\$0.00	\$0.00
SNA	OTA	Sep-09	-	Dec-10	-	\$8.77	-	Sep-09	-	\$0.00	\$8.77	\$0.00	\$0.00
FAT	OTA	Sep-09	-	Jan-11	-	\$3.75	-	Jun-09	-	\$0.15	\$3.60	\$0.00	\$0.00
MSP	OTA	Nov-09	-	Apr-11	-	\$8.00	-	Sep-09	-	\$0.00	\$8.00	\$0.00	\$0.00
TRI	OTA	Jan-09	-	Sep-09	-	\$3.25	-	Sep-09	-	\$0.00	\$3.25	\$0.00	\$0.00
AMA	OTA	Mar-09	-	Jun-11	-	\$8.25	-	Sep-09	-	\$0.00	\$8.25	\$0.00	\$0.00
PTN	OTA	Jul-09	-	Mar-10	-	\$7.25	-	Jul-09	-	\$0.00	\$7.25	\$0.00	\$0.00
Medium Throughput EDS	Purchase	Mar-09	-	Sep-09	-	\$84.74	-	Mar-09	-	\$0.00	\$84.74	\$0.00	\$0.00
Reduced Size EDS	Purchase	Jun-09	Mar-09	Sep-09	-	\$23.00	-	Jan-09	Mar-09	\$19.52	\$3.48	\$0.00	\$13.38
ENR	Install	Oct-09	-	May-10	-	\$1.24	-	Oct-09	-	\$0.00	\$1.24	\$0.00	\$0.00
ORD	Install	Dec-09	-	Jun-10	-	\$1.55	-	Dec-09	-	\$0.00	\$1.55	\$0.00	\$0.00
CNG	Install	Aug-09	Mar-09	Mar-09	-	\$2.16	-	Aug-09	Mar-09	\$2.43	-\$0.27	\$0.00	\$0.23
MCO	Install	Aug-09	Apr-09	Mar-09	-	\$2.65	-	Aug-09	Mar-09	\$0.72	\$1.93	\$0.60	\$0.11
MIA	Install	Sep-09	Apr-09	Apr-09	-	\$2.65	-	Sep-09	Mar-09	\$1.12	\$1.51	\$0.00	\$0.00
IAE	Install	Dec-09	-	May-10	-	\$1.55	-	Dec-09	-	\$0.00	\$1.55	\$0.00	\$0.00
ACS	Install	Feb-09	-	Feb-09	-	\$0.12	-	Feb-09	-	\$0.02	\$0.10	\$0.00	\$0.00
SAT	Install	Oct-09	-	Aug-10	-	\$2.42	-	Oct-09	-	\$0.00	\$2.42	\$0.00	\$0.00
PTN	Install	Dec-09	-	Jun-10	-	\$0.92	-	Dec-09	-	\$0.00	\$0.92	\$0.00	\$0.00
SJC	Install	Jul-09 & Jan-10	-	Mar-10 & Sep-10	-	\$2.92	-	Jul-09	-	\$0.00	\$2.92	\$0.00	\$0.00
AMA	Install	May-09	-	May-09	-	\$0.82	-	May-09	-	\$0.00	\$0.82	\$0.00	\$0.00
MFR	Install	Feb-09	Feb-09	Feb-09	-	\$1.04	-	May-09	Feb-09	\$0.76	\$0.28	\$0.00	\$0.00
TLJ	Install	Nov-09	-	Jun-10	-	\$1.03	-	Nov-09	-	\$0.00	\$1.03	\$0.00	\$0.00
OGG	Install	Aug-09	-	Mar-10	-	\$1.10	-	Aug-09	-	\$0.00	\$1.10	\$0.00	\$0.00

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix L. EBSP FY 2009 Obligation by Project (continued)

Project	Spend Plan	Project Timelines				Project Cost		Obligation Schedule		Obligation Balances			Expenditures
		Ant. Start Date	Actual Start Date	Ant. End Date	Actual End Date	Initial Dollar Amt.	Revised Dollar Amt.	Planned Obligation	Actual Obligation	Obligated	Unobligated Balance	Anticipated Unobligated	
PHX	Install	Aug-09	-	Mar-09	-	\$0.45	-	Aug-09	-	\$0.00	\$0.45	\$0.00	\$0.00
PNS	Install	Jan-09	-	Mar-09	-	\$0.12	-	Jul-09	-	\$0.00	\$0.09	\$0.00	\$0.00
RDU	Install	Mar-09	-	Oct-09	-	\$0.00	-	Mar-09	-	\$0.00	\$0.00	\$0.00	\$0.00
RNO	Install	Jul-09	-	Jul-09	-	\$0.90	-	Aug-09	-	\$0.00	\$0.90	\$0.00	\$0.00
RQC	Install	May-09	-	May-09	-	\$0.00	-	May-09	-	\$0.00	\$0.00	\$0.00	\$0.00
SAN	Install	Aug-09	Mar-09	Mar-09	-	\$0.24	-	Aug-09	Feb-09	\$0.19	\$0.05	\$0.00	\$0.00
SFO	Install	Jun-09	-	Apr-09	-	\$1.43	-	Jan-09	-	\$0.00	\$1.43	\$0.00	\$0.00
SNA	Install	Nov-09	-	Jun-09	-	\$2.11	-	Nov-09	-	\$0.00	\$2.11	\$0.00	\$0.00
LSE	Install	May-09	-	May-09	-	\$0.08	-	May-09	-	\$0.00	\$0.08	\$0.00	\$0.00
PYT	Install	Aug-09	-	Aug-09	-	\$0.08	-	Aug-09	-	\$0.00	\$0.08	\$0.00	\$0.00
SMX	Install	Jun-09	-	Jun-09	-	\$0.08	-	Jun-09	-	\$0.00	\$0.08	\$0.00	\$0.00
FTO	Install	Jun-09	-	Jun-09	-	\$0.08	-	Jun-09	-	\$0.00	\$0.08	\$0.00	\$0.00
OPT	Install	Jun-09	-	Jun-09	-	\$0.08	-	Jun-09	-	\$0.00	\$0.08	\$0.00	\$0.00
MKK	Install	Jun-09	-	Jun-09	-	\$0.08	-	Jun-09	-	\$0.00	\$0.08	\$0.00	\$0.00
HLN	Install	Jun-09	-	Jun-09	-	\$0.08	-	Jun-09	-	\$0.00	\$0.08	\$0.00	\$0.00
CHA	Install	Mar-09	-	Mar-09	-	\$0.08	-	Mar-09	-	\$0.00	\$0.08	\$0.00	\$0.00
CHS	Install	Feb-09	-	Feb-09	-	\$0.26	-	Feb-09	-	\$0.00	\$0.26	\$0.00	\$0.00
CMJ	Install	Apr-09	-	Apr-09	-	\$0.08	-	Apr-09	-	\$0.00	\$0.08	\$0.00	\$0.00
SUN	Install	Apr-09	-	Apr-09	-	\$0.08	-	Apr-09	-	\$0.01	\$0.07	\$0.00	\$0.00
GUC	Install	May-09	-	May-09	-	\$0.08	-	May-09	-	\$0.00	\$0.08	\$0.00	\$0.00
SAN-RS	Install	Apr-09	-	Apr-09	-	\$0.60	-	Apr-09	-	\$0.00	\$0.60	\$0.00	\$0.00
PHL-RS	Install	May-09	-	May-09	-	\$0.89	-	May-09	-	\$0.00	\$0.89	\$0.00	\$0.00
HON	Install	May-09	-	May-09	-	\$1.24	-	May-09	-	\$0.00	\$1.24	\$0.00	\$0.00
BCE	Install	Jun-09	-	Jun-09	-	\$0.72	-	Jun-09	-	\$0.00	\$0.72	\$0.00	\$0.00
ASB**	Install	Replaced with SBA	-	Replaced with SBA	-	\$0.00	-	Project cancelled and replaced with SBA	-	\$0.00	\$0.00	\$0.00	\$0.00
SBA**	Install	Jul-09	-	Jul-09	-	\$0.72	-	Jul-09	-	\$0.00	\$0.72	\$0.00	\$0.00
TUS	Install	Mar-09	-	Mar-09	-	\$0.33	-	Mar-09	-	\$0.00	\$0.33	\$0.00	\$0.00
UTA	Install	Jun-09	-	Jun-09	-	\$0.08	-	Jun-09	-	\$0.01	\$0.07	\$0.00	\$0.00
KDM	Install	Feb-09	-	Feb-09	-	\$0.72	-	Feb-09	-	\$0.00	\$0.72	\$0.00	\$0.00
Recap	Install	Ongoing thru Sept	-	Sep-09	-	\$5.00	-	Ongoing thru Sept	-	\$0.00	\$5.00	\$0.00	\$0.00

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix L: EBSP FY 2009 Obligation by Project (continued)

Project	Spend Plan	Project Timelines				Project Cost		Obligation Schedule		Obligation Balances			Expenditures
		Ant. Start Date	Actual Start Date	Ant. End Date	Actual End Date	Initial Dollar Amt.	Revised Dollar Amt.	Planned Obligation	Actual Obligation	Obligated	Unobligated Balance	Anticipated Unobligated	
COTR/Engineering Initiatives	T&E	Ongoing thru Sept	-	Sep-09	-	\$25.00	17.00	Ongoing thru Sept	n/a	\$2.07	\$15.53	\$3.80	0.00
STIP	T&E	Ongoing thru Sept	-	Sep-09	-	\$8.00	-	Ongoing thru Sept	n/a	\$1.00	\$6.97	\$0.00	0.00
ASP	T&E	Ongoing thru Sept	-	Sep-09	-	\$5.00	-	Ongoing thru Sept	n/a	\$0.00	\$5.00	\$0.00	0.00
CE	T&E	Ongoing thru Sept	-	Sep-09	-	\$2.00	-	Ongoing thru Sept	n/a	\$0.00	\$2.00	\$0.00	0.00
Ops & Compliance, Program Support, Engineering Support, TSIF Support, & PC&B	P,O & M	Ongoing thru Sept	-	Sep-09	-	\$74.90	\$0.06	Ongoing thru Sept	n/a	\$30.50	\$39.58	\$0.00	0.00
TSIF Bridging Purchase	P,O & M	Ongoing thru Sept	-	Sep-09	-	\$7.40	-	Ongoing thru Sept	n/a	\$0.00	\$0.00	\$0.00	0.00

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix M. EBSF ARRA Obligation by Project

Project	Spend Plan	Project Timelines				Project Costs		Obligation Schedule		Obligation Balances			Repayments
		Ant. Start Date	Actual Start Date	Ant. End Date	Actual End Date	Initial Dollar Amt.	Revised Dollar Amt.	Planned Obligation	Actual Obligation	Obligated	Unobligated Balance	Anticipated Unobligated	
HOL	OTA	Jul-09	-	Aug-10	-	\$43.50	\$24.50	Jul-09	-	\$0.00	\$24.50	\$0.00	-
OCE	OTA	Aug-09	-	Nov-10	-	\$14.50	\$7.20	Aug-09	-	\$0.00	\$7.20	\$0.00	-
PHL	OTA	Jun-09	-	Aug-10	-	\$33.00	\$26.00	Jun-09	Jun-09	\$26.00	\$0.00	\$0.00	-
SHC	OTA	Sep-09	-	Dec-10	-	\$11.00	\$23.94	Sep-09	-	\$0.00	\$23.94	\$0.00	-
TLH	OTA	-	-	-	-	\$15.00	-	-	-	-	-	-	-
PWM	OTA	Aug-09	-	Nov-10	-	\$13.30	\$13.50	Aug-09	-	\$0.00	\$13.50	\$0.00	-
SFO	OTA	Jan-09	-	Aug-10	-	\$30.00	\$15.35	Jan-09	Jul-09	\$15.35	\$0.00	\$0.00	-
SMP	OTA	Jul-09	-	Aug-10	-	\$53.00	\$11.34	Jul-09	-	\$0.00	\$11.34	\$0.00	-
7AC	OTA	Jun-09	-	Aug-10	-	\$8.00	\$0.31	Jun-09	Jun-09	\$0.31	\$0.00	\$0.00	-
RSV	OTA	Sep-09	-	Dec-10	-	\$27.50	\$1.50	Sep-09	-	\$0.00	\$1.50	\$0.00	-
MCO	OTA	Jul-09	-	Aug-10	-	\$104.50	\$14.93	Jul-09	Jul-09	\$14.93	\$0.00	\$0.00	-
MCO	OTA	Sep-09	-	Dec-10	-	-	\$13.80	Sep-09	-	\$0.00	\$13.80	\$0.00	-
SAT	OTA	Nov-09	-	Dec-11	-	\$14.39	\$0.00	Sep-09	-	\$0.00	\$14.39	\$0.00	-
BAY	OTA	Aug-09	-	Nov-10	-	\$20.00	\$5.70	Aug-09	-	\$0.00	\$5.70	\$0.00	-
ATL	OTA	Sep-09	-	Dec-10	-	\$54.20	\$21.20	Sep-09	-	\$0.00	\$21.20	\$0.00	-
MSY	OTA	Dec-09	-	Apr-11	-	\$14.55	\$24.97	Dec-09	-	\$0.00	\$24.97	\$0.00	-
CMH	OTA	Sep-09	-	Dec-10	-	\$60.00	\$26.50	Sep-09	-	\$0.00	\$26.50	\$0.00	-
STL	OTA	Sep-09	-	Dec-10	-	\$0.00	\$31.50	Sep-09	-	\$0.00	\$31.50	\$0.00	-
IAD	OTA	Sep-09	-	Dec-10	-	\$0.00	\$148.91	Sep-09	-	\$0.00	\$148.91	\$0.00	-
CYD	OTA	Sep-09	-	Dec-10	-	\$0.00	\$0.35	Sep-09	-	\$0.00	\$0.35	\$0.00	-
HOU	OTA	Sep-09	-	Dec-10	-	\$0.00	\$0.51	Sep-09	-	\$0.00	\$0.51	\$0.00	-
PRE	OTA	Oct-09	-	Jan-11	-	\$0.00	\$0.63	Sep-09	-	\$0.00	\$0.63	\$0.00	-
BZN	OTA	Dec-09	-	Apr-11	-	\$0.00	\$0.80	Dec-09	-	\$0.00	\$0.80	\$0.00	-
TUL	OTA	Dec-09	-	Mar-11	-	\$0.00	\$4.72	Dec-09	-	\$0.00	\$4.72	\$0.00	-
CLY	OTA	Jan-09	-	Mar-11	-	\$0.00	\$31.78	Jan-09	-	\$0.00	\$31.78	\$0.00	-
COS	OTA	Jan-09	-	Mar-11	-	\$0.00	\$7.41	Jan-09	-	\$0.00	\$7.41	\$0.00	-
LIT	OTA	Nov-09	-	Feb-11	-	\$0.00	\$8.96	Nov-09	-	\$0.00	\$8.96	\$0.00	-
Reduced Spend BBS	Purchase	Ongoing thru Sept	May-09	Sep-09	-	\$64.20	\$94.20	Ongoing thru Sept	n/a	\$47.50	\$46.70	\$0.00	\$17.50
ASP	T&E	Ongoing thru Sept	-	Sep-09	-	\$2.20	\$40.60	Ongoing thru Sept	n/a	\$1.40	\$39.20	\$0.00	\$1.40
Ops & Compliance, Program Support, Engineering Support, TSIF Support, & PC&B	P,O & M	Ongoing thru Sept	-	Sep-09	-	\$32.00	\$34.65	Ongoing thru Sept	n/a	\$0.00	\$34.65	\$0.00	-

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix N. EBSP FY 2009 Summary Spend Plan

Summary

Section	\$ in Millions
Program Operations and Management	\$97.5
Letters of Intent (LOI)	\$200.0
Other Transaction Agreement (OTA) – New Facility Modification Agreement Projects	\$67.3
Explosives Detection Systems (EDS) Purchase and Install	\$146.6
Technology/Engineering Initiatives	\$32.6
Total	\$544.0

Program Operations and Management

Project Description	Total TSA FY09 Project Cost
Operations and Compliance/Interim Solutions	
- Moves, Adds and Changes	\$7.5
- Equipment Warehousing	\$3.5
Program Support	
- Program, Resource and Data Management Services	\$16.0
- Testing Services	\$18.1
- Audits, Travel, Training and Certification	\$1.2
Engineering Support	
- Integration and Installation Management	\$13.5

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix N. EBSP FY 2009 Summary Spend Plan (continued)

Project Description	Total TSA FY 2009 Project Cost
Engineering Technical and Design Support	\$10.5
TSA Systems Integration Facility (TSIF) Support	\$4.8
TSIF Building Purchase	\$7.4
Personnel Compensation and Benefits	\$15.0
Total	\$97.5

LOI Projects

Airport	Scope of Work	TSA Cost Share	Total TSA FY 2009 Project Cost
JFK	LOI funding for the airport to construct a Checked Baggage Inspection System (CBIS) for Terminals 2, 3, 4 and 7	90%	\$78.0
EWR	LOI funding for the airport to construct a CBIS for Terminals A, B and C	90%	\$60.0
LGA	LOI funding for the airport to construct a CBIS for Terminals USAir and Central Terminal Building	90%	\$62.0
Total LOI Projects			\$200.0

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix N. EBSP FY 2009 Summary Spend Plan (continued)

OTA – New Facility Modification Agreement Projects

Airport	Scope of Work	TSA Cost Share*	Total TSA FY09 Project Cost
ORD	OTA funding for the airport to construct a CBIS for Terminal 1-B South	90%	\$19.8
ICT	OTA funding for the airport to construct a CBIS for Terminal Main	95%	\$8.25
SAT	OTA funding for the airport to construct a CBIS for Terminal 1/B (funded via American Recovery and Reinvestment Act)	90%	\$0.0
FAT	OTA funding for the airport to construct a CBIS for Terminal Main	95%	\$3.75
MSP	OTA funding for the airport to construct a CBIS for the Lindbergh Terminal	90%	\$8.0
TRI	OTA funding for the airport to construct a CBIS for Terminal Main	95%	\$3.25
AMA	OTA funding for the airport to construct a CBIS for Terminal Main	95%	\$8.25
PFN	OTA funding for the airport to construct a CBIS for New Terminal	95%	\$7.25
SNA	OTA funding for the airport to construct a CBIS for Terminals A and B	90%	\$8.77
Total OTA			\$67.3

* TSA's cost share in this table is 90 percent for a project at a medium or large hub airport and 95 percent for a project at a small and non-hub airport.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix N. EBSP FY 2009 Summary Spend Plan (continued)

FY 2009 EDS Purchase and Install Projects

Airport	Scope of Work	Purchase	Deployment	TSA Cost Share*	Total TSA FY 2009 Project Cost
EWR	Purchase, install, integrate, network and test (3) Medium Speed EDS	\$3.24	\$1.24	100%	\$4.48
ORD	Purchase, install, integrate, network and test (4) Medium Speed EDS for Terminal 1 B-South	\$4.32	\$1.55	100%	\$5.87
CVG	Purchase, install, integrate, network and test(5) Medium Speed EDS for Terminal 3	\$5.40	\$2.16	100%	\$7.56
MCO	Purchase, install, integrate, network and test (7) Medium Speed EDS for Terminal Central East	\$7.56	\$2.65	100%	\$10.21
MIA	Purchase, install, integrate, network and test (8) Medium Speed EDS for Terminal East/Cruise Matrix	\$8.64	\$2.63	100%	\$11.27
IAH	Purchase, install, integrate, network and test (4) Medium Speed EDS for Terminal D	\$4.32	\$1.55	100%	\$5.87
ACK	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.42	\$0.12	100%	\$0.54
SAT	Purchase, install, integrate, network and test (7) Medium Speed EDS for Terminal 1/B	\$7.56	\$2.42	100%	\$9.98
PFN	Purchase, install, integrate, network and test (2) Medium Speed EDS for Terminal New	\$2.16	\$0.92	100%	\$3.08

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix N. EBSP FY 2009 Summary Spend Plan (continued)

Airport	Scope of Work	Purchase	Deployment	TSA Cost Share*	Total TSA FY 2009 Project Cost
SJC	Purchase, install, integrate, network and test (8) Medium Speed EDS for Terminal A/B	\$9.72	\$2.92	100%	\$12.64
AMA	Purchase, install, integrate, network and test (2) Reduced Size EDS for Terminal Main	\$0.84	\$0.82	100%	\$1.66
MFR	Purchase, install, integrate, network and test (2) Reduced Size EDS for Terminal Main	\$0.84	\$1.04	100%	\$1.88
TLH	Purchase, install, integrate, network and test (2) Medium Speed EDS for Terminal Main	\$2.16	\$1.03	100%	\$3.19
OGG	Install, integrate, network, and test (3) Medium Speed EDS for Terminal Main	\$-	\$1.10	100%	\$1.10
PHX	Purchase, install, integrate, network and test (1) Medium Speed EDS for Terminal 4	\$1.08	\$0.45	100%	\$1.53
PNS	Purchase, install, integrate, network and test (1) Medium Speed EDS for Terminal Main	\$0.42	\$0.12	100%	\$0.54
RDU	Purchase of (2) Medium Speed EDS for Terminal C West	\$2.16	\$-	100%	\$2.16
RNO	Install, integrate, network and test (3) Reduced Size EDS for Terminal Main	\$-	\$0.90	100%	\$0.90
ROC	Purchase of (6) Reduced Size EDS for Terminal Main	\$2.53	\$-	100%	\$2.53

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix N. EBSP FY 2009 Summary Spend Plan (continued)

Airport	Scope of Work	Purchase	Deployment	TSA Cost Share*	Total TSA FY 2009 Project Cost
SAN	Purchase, install, integrate, network and test (1) Medium Speed EDS for Terminal 2 East	\$1.08	\$0.24	100%	\$1.32
SFO	Purchase, install, integrate, network and test (4) Medium Speed EDS for Terminal C	\$4.32	\$1.43	100%	\$5.75
SNA	Purchase, install, integrate, network and test (4) Medium Speed EDS for Terminal C	\$4.32	\$2.11	100%	\$6.43
LSE	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.42	\$0.08	100%	\$0.50
PIT	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.42	\$0.08	100%	\$0.50
SMX	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.42	\$0.08	100%	\$0.50
ITO	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.42	\$0.08	100%	\$0.50
GPI	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.42	\$0.08	100%	\$0.50
MKK	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.42	\$0.08	100%	\$0.50
HLN	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.42	\$0.08	100%	\$0.50

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix N. EBSP FY 2009 Summary Spend Plan (continued)

Airport	Scope of Work	Purchase	Deployment	TSA Cost Share*	Total TSA FY 2009 Project Cost
CHA	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.42	\$0.08	100%	\$0.50
CHS	Purchase, install and test (3) Reduced Size EDS for Terminal Main	\$1.26	\$0.26	100%	\$1.52
CMI	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.42	\$0.08	100%	\$0.50
SUN	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.42	\$0.08	100%	\$0.50
GUC	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.42	\$0.08	100%	\$0.50
SAN-RS	Purchase, install, integrate, network and test (5) Reduced Size EDS for Terminal I	\$2.10	\$0.60	100%	\$2.70
PHL-RS	Purchase, install, integrate, network and test (3) Reduced Size EDS for Terminal B/C	\$1.26	\$0.89	100%	\$2.16
HDN	Install, integrate, network, and test (3) Reduced Size EDS for Terminal Main	\$-	\$1.24	100%	\$1.24
EGE	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.84	\$0.72	100%	\$1.56
ASE**	Purchase, install, integrate, network and test (2) Reduced Size EDS for Terminal Main				
SBA**	Purchase, install, integrate, network and test (2) Reduced Size EDS for Terminal Main	\$0.84	\$0.72	100%	\$1.56

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix N. EBSP FY 2009 Summary Spend Plan (continued)

Airport	Scope of Work	Purchase	Deployment	TSA Cost Share*	Total TSA FY 2009 Project Cost
TUS	Purchase, install, integrate, network and test (2) Reduced Size EDS for Terminal Main	\$1.68	\$0.33	100%	\$2.02
UTA	Purchase, install, integrate, network and test (2) Reduced Size EDS for Terminal Main	\$0.42	\$0.08	100%	\$0.5
RDM	Purchase, install, integrate, network and test (2) Reduced Size EDS for Terminal Main	\$0.84	\$0.72	100%	\$1.56
Recapitalization		\$20.75	\$5.0	100%	\$25.75
Total Purchase and Install		\$107.7	\$38.8		\$146.6

* TSA funds 100 percent of the Purchase and Install costs associated with each project

** ASE was canceled and replaced with SBA

Technology/Engineering Initiatives

Project Description	Total TSA FY 2009 Project Cost
Contracting Officer's Technical Representative/Engineering Initiatives	\$17.6
Security Technology Integrated Program	\$8.0
Advanced Surveillance Program	\$5.0
Operations Integration	\$2.0
Total	\$32.6

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix O. EBSP ARRA Summary Spend Plan

Summary

Section	Total	Revised Total*
Program Operations and Management	\$32.0	\$54.85
OTA – New Facility Modification Agreement Projects	\$598.1	\$499.2
EDS Purchase and Install	\$64.2	\$94.2
Technology/Engineering Initiatives	\$5.7	\$40.6
Total	\$700.0	\$688.85

*Revised Total: \$11 million shifted from EDS to PSP for ASP/CCTV projects

Program Operations and Management

Project Description	Total TSA FY 2009 ARRA Project Cost	Revised TSA FY 2009 ARRA Project Cost
Operations and Compliance/Interim Solutions		
- Moves, Adds and Changes	\$8.0	\$7.85
Program Support		
- Program, Resource and Data Management Services	\$6.8	\$10.0
- Testing Services	\$3.0	\$5.3
Engineering Support		
- Integration and Installation Management	\$7.8	\$24.8
- Engineering Technical and Design Support	\$2.6	\$3.1
Personnel Compensation and Benefits	\$3.8	\$3.8
Total	\$32.0	\$54.85

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix O. EBSP ARRA Summary Spend Plan (continued)

OTA – New Facility Modification Agreement Projects

Airport	Scope of Work	TSA Cost Share	Original TSA FY 2009 ARRA Project Cost	Revised TSA FY 2009 ARRA Project Cost
HNL	OTA funding for the airport to construct a Checked Baggage Inspection System (CBIS) for Terminals 4, 5, 6, 7, 8	90%	\$43.50	\$24.50
OGG	OTA funding for the airport to construct a CBIS for Main Terminal	90%	\$18.50	\$7.20
PHL	OTA funding for the airport to construct a CBIS for Terminal A East	90%	\$53.00	\$26.60
SJC	OTA funding for the airport to construct a CBIS for Terminal B	90%	\$31.00	\$23.94
TLH	OTA funding for the airport to construct a CBIS for Main Terminal (canceled)	95%	\$15.00	-
PWM	OTA funding for the airport to construct a CBIS for Main Terminal	95%	\$13.30	\$13.50
SFO	OTA funding for the airport to construct a CBIS for Terminal 2	90%	\$30.00	\$15.35
SMF	OTA funding for the airport to construct a CBIS for Terminal B	90%	\$53.00	\$11.34

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix O. EBSP ARRA Summary Spend Plan (continued)

Airport	Scope of Work	TSA Cost Share	Original TSA FY 2009 ARRA Project Cost	Revised TSA FY 2009 ARRA Project Cost
JAC	OTA funding for the airport to construct a CBIS for Main Terminal	95%	\$8.80	\$6.21
HSV	OTA funding for the airport to construct a CBIS for Main Terminal	95%	\$27.50	\$1.50
MCO	OTA funding for the airport to construct a CBIS for East Terminal	90%	\$104.50	\$14.93
MCO	OTA funding for the airport to construct a CBIS for Disney Terminal		-	\$13.80
SNA	OTA funding for the airport to construct a CBIS for Terminals A and B (funded via FY09)	90%	\$51.30	
DAY	OTA funding for the airport to construct a CBIS for Main Terminal	95%	\$20.00	\$9.70
ATL	OTA funding for the airport to construct a CBIS for Main Terminal	90%	\$54.20	\$21.20
MSY	OTA funding for the airport to construct a CBIS for Main Terminal	90%	\$14.50	\$24.97

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix O. EBSP ARRA Summary Spend Plan (continued)

Airport	Scope of Work	TSA Cost Share	Original TSA FY 2009 ARRA Project Cost	Revised TSA FY 2009 ARRA Project Cost
CMH	OTA funding for the airport to construct a CBIS for Main Terminal	90%	\$60.00	\$26.50
STL	OTA funding for the airport to construct a CBIS for Main Terminal	90%	\$0.00	\$31.50
IAD	OTA funding for the airport to construct a CBIS for Main Terminal	90%	\$0.00	\$148.91
COD	OTA funding for the airport to construct a CBIS for Main Terminal	95%	\$0.00	\$0.35
HOU	OTA funding for the airport to construct a CBIS for Main Terminal	90%	\$0.00	\$0.51
PIE	OTA funding for the airport to construct a CBIS for Main Terminal	95%	\$0.00	\$0.63
BZN	OTA funding for the airport to construct a CBIS for Main Terminal	95%	\$0.00	\$6.80
TUL	OTA funding for the airport to construct a CBIS for Main Terminal	95%	\$0.00	\$4.72

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix O. EBSP ARRA Summary Spend Plan (continued)

Airport	Scope of Work	TSA Cost Share	Original TSA FY 2009 ARRA Project Cost	Revised TSA FY 2009 ARRA Project Cost
CLT	OTA funding for the airport to construct a CBIS for Main Terminal	90%	\$0.00	\$33.78
COS	OTA funding for the airport to construct a CBIS for Main Terminal	95%	\$0.00	\$7.41
LIT	OTA funding for the airport to construct a CBIS for Main Terminal	95%	\$0.0	\$8.96
SAT	OTA funding for the airport to construct a CBIS for Terminal 1/B	90%	\$0	\$14.39
Total			\$598.10	\$499.20

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix O. EBSP ARRA Summary Spend Plan (continued)

OTA – New Facility Modification Agreement Projects Reason for Change to Project Costs

Airport	Reason for Change
HNL	Cost validation
OGG	Cost to complete and cost validation
PHL	Cost validation
SJC	Cost validation
TLH	Airport Canceled Project
PWM	Cost validation
SFO	Cost validation
SMF	Cost validation after de-scoping of project
JAC	Cost validation
HSV	Cost validation
MCO	Cost validation
MCO	Of the \$104.5 million, Phase II has an Original Cost Estimate of \$13.2 million
SNA	Cost validation
DAY	Cost validation

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix O. EBSP ARRA Summary Spend Plan (continued)

Airport	Reason for Change
ATL	Cost validation
MSY	Cost validation
CMH	Cost validation
STL	New project
IAD	New project
COD	New project
HOU	New project
PIE	New project
BZN	New project
TUL	New project
CLT	New project
COS	New project
LIT	New project

Original projected costs were based solely on submitted airport applications. Validated projects found airports submitted applications with non-allowable/allocable construction-related costs, design fees and/or construction management.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix O. EBSP ARRA Summary Spend Plan (continued)

Reduced Size EDS

Scope of Work	TSA Cost Share	Total TSA FY 2009 ARRA Project Cost	Revised TSA FY 2009 ARRA Project Cost
Recapitalization	100%	\$43.2	\$58.2
ETD Only Airport	100%	\$21.0	\$36.0
Total		\$64.2	\$94.2

Technology/Engineering Initiatives

Project Description	Total TSA FY 2009 ARRA Project Cost	Revised TSA FY 2009 ARRA Project Cost
Engineering Initiatives	\$3.5	\$0
Advanced Surveillance Program	\$2.2	\$40.6
- Boise Air Terminal/Gowen Field (BOI)	\$0.3	\$0.3
- Ronald Reagan Washington National (DCA)	\$1.1	\$1.1
- Cincinnati/Northern Kentucky International (CVG)	\$1.2	\$1.2
- Spokane International (GEG)	\$0.4	\$0.4
- Gerald R. Ford International (GRR)	\$1.2	\$1.2
- Washington Dulles International (IAD)	\$0	\$5.8
- Will Rogers World (OKC)	\$0	\$4.2
- Chicago Midway International Airport (MDW)	\$0	\$6.8
- Eppley Airfield (OMA)	\$0	\$4.0

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix O. EBSP ARRA Summary Spend Plan (continued)

Project Description	Total TSA FY 2009 ARRA Project Cost	Revised TSA FY 2009 ARRA Project Cost
- <i>James M Cox Dayton International Airport (DAY)</i>	<i>\$0</i>	<i>\$3.0</i>
- <i>Kansas City International (MCI)</i>	<i>\$0</i>	<i>\$5.8</i>
- <i>Adams Field (LIT)</i>	<i>\$0</i>	<i>\$3.0</i>
- <i>Tampa International (TPA)</i>	<i>\$0</i>	<i>\$6.0</i>
Total	\$5.7	\$40.6

Numbers may not add due to rounding.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix P. EBSP FY 2009 Obligation Data

Obligation Schedule

Obligation dates and selected airports are subject to change based on airport schedules and contract negotiations.

Airport	Scope of Work	Project Cost \$ in Millions	Planned Obligation Date
Program Operations and Management			
N/A	Ops Compliance, Program Support, Engineering Support, TSIF Support and P, C and B	\$97.5	Ongoing through Sept-09
LOI Projects			
JFK	LOI Funding for the airport to construct a CBIS for Terminals 2, 3, 4 and 7	\$78.0	May-09
EWR	LOI funding for the airport to construct a CBIS for Terminals A, B and C	\$60.0	May-09
LGA	LOI funding for the airport to construct a CBIS for Terminals USAir and CTB	\$62.0	May-09
EDS Install and Purchase Projects			
EWR	Purchase, install, integrate, network and test (3) Medium Speed EDS	\$4.48	P-Jun-09 I-Oct-09
ORD	Purchase, install, integrate, network and test (4) Medium Speed EDS for Terminal 1B-South	\$5.87	P-Jun-09 I-Dec-09

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix P. EBSP FY 2009 Obligation Data (continued)

Airport	Scope of Work	Project Cost \$ in Millions	Planned Obligation Date
EDS Install and Purchase Projects (continued)			
CVG	Purchase, install, integrate, network and test (5) Medium Speed EDS for Terminal 3	\$7.56	P-Jun-09 1-Aug-09
MCO	Purchase, install, integrate, network and test (7) Medium Speed EDS for Terminal Central East	\$10.21	P-Jun-09 1-Aug-09
MLA	Purchase, install, integrate, network and test (8) Medium Speed EDS for Terminal East/Cruise Matrix	\$11.27	P-Jun-09 1-Sep-09
IAH	Purchase, install, integrate, network and test (4) Medium Speed EDS for Terminal D	\$5.87	P-Jun-09 1-Dec-09
ACK	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.54	P-Jan-09 1-Feb-09
SAT	Purchase, install, integrate, network and test (7) Medium Speed EDS for Terminal 1/B	\$9.98	P-Jun-09 1-Oct-09
PFN	Purchase, install, integrate, network and test (2) Medium Speed EDS for Terminal New	\$3.08	P-Jun-09 1-Dec-09
SJC	Purchase, install, integrate, network and test (8) Medium Speed EDS for Terminal A/B	\$12.64	P-Jun-09 1-Jul-09 Dec-09
AMA	Purchase, install, integrate, network and test (2) Reduced Size EDS for Terminal Main	\$1.66	P-Mar-09 1-May-09
MFR	Purchase, install, integrate, network and test (2) Reduced Size EDS for Terminal Main	\$1.88	P-Jan-09 1-May-09

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix P. EBSP FY09 Obligation Data (continued)

Airport	Scope of Work	Project Cost \$ in Millions	Planned Obligation Date
EDS Install and Purchase Projects (continued)			
TLH	Purchase, install, integrate, network and test (2) Medium Speed EDS for Terminal Main	\$3.19	P-Jun-09 I-Nov-09
OGG	Install, integrate, network and test (3) Medium Speed EDS for Terminal Main	\$1.10	P-warehouse* I-Aug-09
PHX	Purchase, install, integrate, network and test (1) Medium Speed EDS for Terminal 4	\$1.53	P-Jan-09 I-Aug-09
PNS	Purchase, install, integrate, network and test (1) Medium Speed EDS for Terminal Main	\$0.54	P-Jan-09 I-Jul-09
RDU	Purchase of (2) Medium Speed EDS for Terminal C West	\$2.16	P-Sep-09 I-Mar-10
RNO	Install, integrate, network and test (3) Reduced Size EDS for Terminal Main	\$0.90	P-relocation* I-Aug-09
ROC	Purchase of (6) Reduced Size EDS for Terminal Main	\$2.53	P-Mar-09 I-May-09 *
SAN	Purchase, install, integrate, network and test (1) Medium Speed EDS for Terminal 2 East	\$1.32	P-Jan-09 I-Aug-09
SFO	Purchase, install, integrate, network and test (4) Medium Speed EDS for Terminal 2	\$5.75	P-Jun-09 I-Jan-10

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix P. EBSP FY 2009 Obligation Data (continued)

Airport	Scope of Work	Project Cost \$ in Millions	Planned Obligation Date
EDS Install and Purchase Projects (continued)			
SNA	Purchase, install, integrate, network and test (4) Medium Speed EDS for Terminal C	\$6.43	P-Jun-09 I-Nov-09
LSE	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.50	P-Mar-09 I-May-09
PIT	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.50	P-Mar-09 I-Aug-09
SMX	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.50	P-Mar-09 I-Jun-09
ITO	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.50	P-Mar-09 I-Jun-09
GPI	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.50	P-Mar-09 I-Jun-09
MKK	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.50	P-Mar-09 I-Jun-09
HLN	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.50	P-Mar-09 I-Jun-09
CHA	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.50	P-Jan-09 I-Mar-09
CHS	Purchase, install and test (3) Reduced Size EDS for Terminal Main	\$1.52	P-Jan-09 I-Feb-09

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix P. EBSP FY 2009 Obligation Data (continued)

Airport	Scope of Work	Project Cost \$ in Millions	Planned Obligation Date
EDS Install and Purchase Projects (continued)			
CMI	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.50	P-Jan-09 I-Apr-09
SUN	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.50	P-Jan-09 I-Apr-09
GUC	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.50	P-Mar-09 I-May-09
SAN-RS	Purchase, install, integrate, network and test (5) Reduced Size EDS for Terminal 1	\$2.70	P-Jan-09 I-Apr-09
PHL-RS	Purchase, install, integrate, network, and test (3) Reduced Size EDS for Terminal B/C	\$2.16	P-Mar-09 I-May-09
HDN	Install, integrate, network and test (3) Reduced Size EDS for Terminal Main	\$1.24	P-Mar-09 I-May-09
EGE	Purchase, install, integrate, network and test (2) Reduced Size EDS for Terminal Main	\$1.56	P-Mar-09 I-Jun-09
ASE	Purchase, install, integrate, network and test (2) Reduced Size EDS for Terminal Main		Project canceled and replaced with SBA
SBA	Purchase, install, integrate, network and test (2) Reduced Size EDS for Terminal Main	\$1.56	P-Mar-09 I-Jul-09

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix P. EBSP FY 2009 Obligation Data (continued)

Airport	Scope of Work	Project Cost \$ in Millions	Planned Obligation Date
EDS Install and Purchase Projects (continued)			
TUS	Purchase, install, integrate, network and test (4) Reduced Size EDS for Terminal Main	\$2.02	P-Jan-09 I-Mar-09
UTA	Purchase, install, integrate, network and test (1) Reduced Size EDS for Terminal Main	\$0.50	P-Mar-09 I-Jun-09
RDM	Purchase, install, integrate, network and test (3) Reduced Size EDS for Terminal Main	\$1.56	P-Jan-09 I-Feb-09

P = purchase

I = install

DEVIATION FROM ORIGINAL SPEND PLAN

After further evaluation, it was determined the current configuration at the Aspen-Pitkin County/Sardy Field (ASE) airport was sufficient to support the needs of the airport. The passenger throughput did not increase as anticipated. The Santa Barbara Municipal (SBA) airport was identified as an airport with increased throughput and served as a replacement airport for the ASE project. The equipment purchase and installation at SBA was comparable to ASE and there were no significant funding changes. The project timeline and schedule were also closely aligned and caused no changes to the current spend plan.

Airport	Technology Purchases	Project Cost \$ in Millions	Planned Obligation Date
N/A	Medium Throughput GE—March through September L3—September	\$84.74	Mar-09 through Sept-09
N/A	Reduced Size Reveal—January through September L3—September	\$23.00	Jan-09 through Sept-09

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix P. EBSP FY 2009 Obligation Data (continued)

Airport	Scope of Work	Project Cost \$ in millions	Planned Obligation Date
New Facility Modification Agreement Projects			
ORD	OTA funding for the airport to construct a CBIS for Terminal 1-B South	\$19.8	May-09
ICT	OTA funding for the airport to construct a CBIS for Terminal Main	\$8.25	Sep-09
SAT	OTA funding for the airport to construct a CBIS for Terminal 1/B (Funded via ARRA)		
FAT	OTA funding for the airport to construct a CBIS for Terminal Main	\$3.75	Jun-09
MSP	OTA funding for the airport to construct a CBIS for the Lindbergh Terminal	\$8.0	Sep-09
TRI	OTA funding for the airport to construct a CBIS for Terminal Main	\$3.25	Sep-09
AMA	OTA funding for the airport to construct a CBIS for Terminal Main	\$8.25	Sep-09
PFN	OTA funding for the airport to construct a CBIS for New Terminal	\$7.25	Jul-09
SNA	OTA funding for the airport to construct a CBIS for Terminals A and B	\$8.77	Sep-09

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix P. EBSP FY 2009 Obligation Data (continued)

Airport	Scope of Work	Project Cost in millions	Planned Obligation Date
Technology/Engineering Initiatives			
N/A	COTR Initiatives, STIP, ASP, OI and Engineering Initiatives	\$32.6	Ongoing through Sept-09

- Funding provided in FY 2008

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix Q. EBSP ARRA Obligation Data

Obligation Schedule

Airport Other Transactional Agreements	Facility Modification	Planned Month for Obligation
HNL	\$24.50	Aug-09
OGG	\$7.20	Aug-09
PHL	\$26.60	Jun-09
SJC	\$23.94	Sep-09
TLH	-	-
PWM	\$13.50	Aug-09
SFO	\$15.35	Jun-09
SMF	\$11.34	Aug-09
JAC	\$6.21	Jun-09
HSV	\$1.50	Sep-09
MCO (East)	\$14.93	July-09
MCO (Disney)	\$13.80	Sep-09
SNA		
DAY	\$9.70	Aug-09
ATL	\$21.20	Sep-09
MSY	\$24.97	Sept 09, Mar-09
CMH	\$26.50	Sep-09
STL	\$31.50	Sep-09
IAD	\$148.91	Sep-09
COD	\$0.35	Sep-09
HOU	\$0.51	Sep-09
PIE	\$0.63	Oct-09
BZN	\$6.80	Dec-09
TUL	\$4.72	Dec-09
CLT	\$33.78	Jan-10
COS	\$7.41	Jan-10
LIT	\$8.96	Nov-09
SAT	\$14.39	Sep-09
Total	\$499.2 millions	

Obligation dates and selected airports are subject to change based on airport schedules and contract negotiations.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix R. EBSP FY 2009 Milestones

Project Timelines – New Facility Modification Agreement Projects

Project Timelines – LOI Projects

Major Milestones	Estimated Completion Date
La Guardia (LGA)	
Initiate second year of LOI evaluation	Dec-08
Airports submit updated cost information to the Transportation Security Administration (TSA)	Apr-09
Modify existing LOI for additional funding requirements*	Jul-09
Newark Liberty International (EWR)	
Initiate second year of LOI evaluation	Dec-08
Airports submit updated cost information to TSA	Apr-09
Modify existing LOI for additional funding requirements*	Jul-09
John F. Kennedy International (JFK)	
Initiate second year of LOI evaluation	Dec-08
Airports submit updated cost information to TSA	Apr-09
Modify existing LOI for additional funding requirements*	Jul-09

*LOIs require congressional notification 3 days before contract execution.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix R. EBSP FY 2009 Milestones (continued)

Project Timelines – EDS Purchase and Install Projects

Major Milestones	Estimated Completion Date
Newark Liberty International (EWR)	
EDS Deliver	Oct-09
Installation and Integration	Oct-09
Independent Verification and Validation (IV&V)/Commissioning	Mar-10
Live Bag Screening	Apr-10
Decommissioning	May-10
Chicago O'Hare International (ORD)	
EDS Delivery	Dec-09
Installation and Integration	Dec-09
IV&V/Commissioning	Apr-10
Live Bag Screening	May-10
Decommissioning	Jun-10
Cincinnati/Northern Kentucky International (CVG)	
EDS Delivery	Feb-09
Installation and Integration	Aug-09
IV&V/Commissioning	Jan-10
Live Bag Screening	Feb-10
Decommissioning	Mar-10
Orlando International (MCO)	
EDS Delivery	Feb-09
Installation and Integration	Aug-09
IV&V/Commissioning	Jan-10
Live Bag Screening	Feb-10
Decommissioning	Mar-10
Miami International (MIA)	
EDS Delivery	Mar-09
Installation and Integration	Sep-09
IV&V/Commissioning	Feb-10
Live Bag Screening	Mar-10
Decommissioning	Apr-10

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix R. EBSP FY 2009 Milestones (continued)

Project Timelines – EDS Purchase and Install Projects (continued)

Major Milestones	Estimated Completion Date
George Bush Intercontinental/Houston (IAH)	
EDS Delivery	Dec-09
Installation and Integration	Dec-09
IV&V/Commissioning	Mar-10
Live Bag Screening	Apr-10
Decommissioning	May-10
Nantucket Memorial (ACK)	
EDS Delivery	Feb-09
Installation and Integration	Feb-09
Decommissioning	N/A
San Antonio International (SAT)	
EDS Delivery	Oct-09
Installation and Integration	Oct-09
IV&V/Commissioning	Jun-10
Live Bag Screening	Jul-10
Decommissioning	Aug-10
Panama City-Bay County International (PFN)	
EDS Delivery	Dec-09
Installation and Integration	Dec-09
IV&V/Commissioning	Apr-10
Live Bag Screening	May-10
Decommissioning	Jun-10
Norman Y. Mineta San Jose International (SJC)	
EDS Delivery	Jul-09 and Dec-09
Installation and Integration	Jul-09 and Jan-10
IV&V/Commissioning	Jan-10 and Jul-10
Live Bag Screening	Feb-10 and Aug-10
Decommissioning	Mar-10 and Sep-10
Rick Husband Amarillo International (AMA)	
EDS Delivery	May-09
Installation and Integration	May-09
Decommissioning	N/A

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix R. EBSP FY 2009 Milestones (continued)

Project Timelines – EDS Purchase and Install Projects (continued)

Major Milestones	Estimated Completion Date
Rogue Valley International-Medford (MFR)	
EDS Delivery	Feb-09
Installation and Integration	Aug-09
Decommissioning	N/A
Tallahassee Regional (TLH)	
EDS Delivery	Oct-09
Installation and Integration	Nov-09
IV&V/Commissioning	Apr-10
Live Bag Screening	May-10
Decommissioning	Jun-10
Kahului (OGG)	
EDS Delivery	Feb-09
Installation and Integration	Aug-09
IV&V/Commissioning	Jan-10
Live Bag Screening	Feb-10
Decommissioning	Mar-10
Phoenix Sky Harbor International Airport (PHX)	
EDS Delivery	Feb-09
Installation and Integration	Aug-09
IV&V/Commissioning	Jan-10
Live Bag Screening	Feb-10
Decommissioning	Mar-10
Pensacola Regional (PNS)	
EDS Delivery	Jan-09
Installation and Integration	Jul-09
Decommissioning	Mar-10
Raleigh-Durham International (RDU)	
EDS Delivery	Oct-09
Installation and Integration	Mar-10
IV&V/Commissioning	Aug-10
Live Bag Screening	Sep-10
Decommissioning	Oct-10

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix R. EBSP FY 2009 Milestones (continued)

Project Timelines – EDS Purchase and Install Projects (continued)

Major Milestones	Estimated Completion Date
Reno/Tahoe International (RNO)	
EDS Delivery	Jul-09
Installation and Integration	Aug-09
Decommissioning	N/A
Greater Rochester International (ROC)	
EDS Delivery	May-09
Installation and Integration	May-09
Decommissioning	N/A
San Diego International (SAN)	
EDS Delivery	Feb-09
Installation and Integration	Aug-09
IV&V/Commissioning	Jan-10
Live Bag Screening	Feb-10
Decommissioning	Mar-10
San Francisco International (SFO)	
EDS Delivery	Dec-09
Installation and Integration	Jan-10
IV&V/Commissioning	Feb-10
Live Bag Screening	Mar-10
Decommissioning	Apr-10
John Wayne Airport-Orange County (SNA)	
EDS Delivery	Nov-09
Installation and Integration	Nov-09
IV&V/Commissioning	Apr-10
Live Bag Screening	May-10
Decommissioning	Jun-10
La Crosse Municipal (LSE)	
EDS Delivery	May-09
Installation and Integration	May-09
Decommissioning	N/A
Pittsburgh International (PIT)	
EDS Delivery	Aug-09
Installation and Integration	Aug-09
Decommissioning	N/A

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix R. EBSP FY 2009 Milestones (continued)

Project Timelines – EDS Purchase and Install Projects (continued)

Major Milestones	Estimated Completion Date
Santa Maria Public Airport (SMX)	
EDS Delivery	Jun-09
Installation and Integration	Jun-09
Decommissioning	N/A
Hilo International (ITO)	
EDS Delivery	Jun-09
Installation and Integration	Jun-09
Decommissioning	N/A
Glacier Park International (GPI)	
EDS Delivery	Jun-09
Installation and Integration	Jun-09
Decommissioning	N/A
Molokai Airport (MKK)	
EDS Delivery	Jun-09
Installation and Integration	Jun-09
Decommissioning	N/A
Helena Regional (HLN)	
EDS Delivery	Jun-09
Installation and Integration	Jun-09
Decommissioning	N/A
Lovell Field (CHA)	
EDS Delivery	Mar-09
Installation and Integration	Mar-09
Decommissioning	N/A
Charleston AFB/International (CHS)	
EDS Delivery	Feb-09
Installation and Integration	Feb-09
Decommissioning	N/A
University of Illinois-Willard (CMI)	
EDS Delivery	Apr-09
Installation and Integration	Apr-09
Decommissioning	N/A

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix R. EBSP FY 2009 Milestones (continued)

Project Timelines – EDS Purchase and Install Projects (continued)

Major Milestones	Estimated Completion Date
Friedman Memorial (SUN)	
EDS Delivery	Apr-09
Installation and Integration	Apr-09
Decommissioning	N/A
Gunnison-Crested Butte Regional (GUC)	
EDS Delivery	May-09
Installation and Integration	May-09
Decommissioning	N/A
San Diego International (SAN-RS)	
EDS Delivery	Apr-09
Installation and Integration	Apr-09
Decommissioning	N/A
Philadelphia International (PHL)	
EDS Delivery	May-09
Installation and Integration	May-09
Decommissioning	N/A
Yampa Valley (HDN)	
EDS Delivery	May-09
Installation and Integration	May-09
Decommissioning	N/A
EDS Delivery	Jun-09
Eagle County Regional (EGE)	
EDS Delivery	Jun-09
Installation and Integration	Jun-09
Decommissioning	N/A
Aspen-Pitkin County/Sardy Field (ASE)	
EDS Delivery	Project canceled
Installation and Integration	Replaced with SBA
Decommissioning	
Santa Barbara Municipal (SBA)	
EDS Delivery	Jun-09
Installation and Integration	Jul-09
Decommissioning	N/A

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix R. EBSP FY 2009 Milestones (continued)

Project Timelines – EDS Purchase and Install Projects (continued)

Major Milestones	Estimated Completion Date
Tucson International (TUS)	
EDS Delivery	Mar-09
Installation and Integration	Mar-09
Decommissioning	N/A
Tunica Municipal (UTA)	
EDS Delivery	Jun-09
Installation and Integration	Jun-09
Decommissioning	N/A
Roberts Field (RDM)	
EDS Delivery	Feb-09
Installation and Integration	Feb-09
Decommissioning	N/A

Standalone EDS equipment is tested at time of delivery. The EDS equipment is usually operational 1 week after installation and testing. Standalone equipment only requires a decommissioning when a replacement is delivered. When additional units are delivered, no decommissioning is necessary.

An airport's construction schedule generally affects the delivery of the TSA equipment and is out of TSA's control. When an airport construction schedule slips, delivery timelines are adjusted accordingly.

Airport accepts delivery of equipment, depending on construction schedule. The equipment is typically not operational for another 3-6 months for inline systems and 1 week for standalone EDS equipment after installation, depending on airport's schedule. TSA awards a delivery order to the Original Equipment Manufacturer for services.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix R. EBSP FY 2009 Milestones (continued)

Project Timelines – New Facility Modification Agreement Projects

Major Milestones	Estimated Completion Date
Chicago O'Hare International (ORD)	
Notification letter sent to airport	February 10, 2009
Draft other transaction agreement (OTA) sent to airport to review the terms and conditions	March 22, 2009
Airports submit updated cost information to TSA	February 19, 2009
Cost validations updated based on information provided by the airport	April 3, 2009
Negotiation meetings scheduled with the airport	April 28, 2009
Negotiations completed and OTA executed	May 2009
Wichita Mid-Continent (ICT)	
Notification letter sent to airport	February 10, 2009
Draft OTA sent to airport to review the terms and conditions	March 22, 2009
Airports submit updated cost information to TSA	February 27, 2009
Cost validations updated based on information provided by the airport	late April 2009
Negotiation meetings scheduled with the airport	June 2009
Negotiations completed and OTA executed	September 2009
Fresno Yosemite International (FAT)	
Notification letter sent to airport	February 23, 2009
Draft OTA sent to airport to review the terms and conditions	February 9, 2009
Airports submit updated cost information to TSA	February 11, 2009
Cost validations updated based on information provided by the airport	March 31, 2009
Negotiation meetings scheduled with the airport	May 2009
Negotiations completed and OTA executed	June 2009

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix R. EBSP FY 2009 Milestones (continued)

Project Timelines – New Facility Modification Agreement Projects (continued)

Major Milestones	Estimated Completion Date
Minneapolis-St. Paul International/Wold-Chamberlain (MSP)	
Notification letter sent to airport	February 10, 2009
Draft OTA sent to airport to review the terms and conditions	March 22, 2009
Airports submit updated cost information to TSA	April 1, 2009
Cost validations updated based on information provided by the airport	April 3, 2009
Negotiation meetings scheduled with the airport	June 2009
Negotiations completed and OTA executed	September 2009
Tri-Cities Regional TN/VA (TRI)	
Notification letter sent to airport	February 10, 2009
Draft OTA sent to airport to review the terms and conditions	March 13, 2009
Airports submit updated cost information to TSA	late March 2009
Cost validations updated based on information provided by the airport	April 9, 2009
Negotiation meetings scheduled with the airport	April 28, 2009
Negotiations completed and OTA executed	September 2009
Rick Husband Amarillo International (AMA)	
Notification letter sent to airport	February 10, 2009
Draft OTA sent to airport to review the terms and conditions	April 6, 2009
Airports submit updated cost information to TSA	February 24, 2009
Cost validations updated based on information provided by the airport	March 25, 2009
Negotiation meetings scheduled with the airport	April 28, 2009
Negotiations completed and OTA executed	September 2009

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix R. EBSP FY 2009 Milestones (continued)

Project Timelines – New Facility Modification Agreement Projects (continued)

Major Milestones	Estimated Completion Date
Panama City-Bay County International (PFN)	
Notification letter sent to airport	February 9, 2009
Draft OTA sent to airport to review the terms and conditions	February 9, 2009
Airports submit updated cost information to TSA	March 20, 2009
Cost validations updated based on information provided by the airport	April 9, 2009
Negotiation meetings scheduled with the airport	June 2009
Negotiations completed and OTA executed	July 2009
John Wayne Airport-Orange County (SNA)	
Notification letter sent to airport	March 2009
Draft OTA sent to airport to review the terms and conditions	mid March 2009
Airports submit updated cost information to TSA	early April 2009
Cost validations updated based on information provided by the airport	mid April 2009
Negotiation meetings scheduled with the airport	early September 2009
Negotiations completed and OTA executed	Late September 2009

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix S. EBSP ARRA Milestones

Project Timelines -- New Facility Modification Agreement Projects

Major Milestones	Estimated Completion Date
Honolulu International Airport (HNL)	
Notification letter sent to airport	March 2009
Draft other transaction agreement (OTA) sent to airport to review the terms and conditions	mid March 2009
Airports submit updated cost information to Transportation Security Administration (TSA)	late March 2009
Cost validations updated based on information provided by the airport	mid April 2009
Negotiation meetings scheduled with the airport	early June 2009
Negotiations completed and OTA executed	August 2009
Kahului Airport (OGG)	
Notification letter sent to airport	March 2009
Draft OTA sent to airport to review the terms and conditions	early March 2009
Airports submit updated cost information to TSA	early March 2009
Cost validations updated based on information provided by the airport	mid March 2009
Negotiation meetings scheduled with the airport	early June 2009
Negotiations completed and OTA executed	late August 2009
Philadelphia International Airport (PHL)	
Notification letter sent to airport	March 2009
Draft OTA sent to airport to review the terms and conditions	mid March 2009
Airports submit updated cost information to TSA	late March 2009
Cost validations updated based on information provided by the airport	mid April 2009
Negotiation meetings scheduled with the airport	early May 2009
Negotiations completed and OTA executed	mid June 2009

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix S. EBSP ARRA Milestones (continued)

Project Timelines – New Facility Modification Agreement Projects (continued)

Major Milestones	Estimated Completion Date
Normal Y. Mineta San Jose International Airport (SJC)	
Notification letter sent to airport	March 2009
Draft OTA sent to airport to review the terms and conditions	mid March 2009
Airports submit updated cost information to TSA	mid March 2009
Cost validations updated based on information provided by the airport	early May 2009
Negotiation meetings scheduled with the airport	late June 2009
Negotiations completed and OTA executed	late September 2009
Tallahassee Regional Airport (TLH)	
Notification letter sent to airport	March 2009
Draft OTA sent to airport to review the terms and conditions	mid March 2009
Airports submit updated cost information to TSA	early April 2009
Cost validations updated based on information provided by the airport	mid April 2009
Negotiation meetings scheduled with the airport	Project canceled by airport
Negotiations completed and OTA executed	N/A
Portland International Jetport (PWM)	
Notification letter sent to airport	March 2009
Draft OTA sent to airport to review the terms and conditions	mid March 2009
Airports submit updated cost information to TSA	mid March 2009
Cost validations updated based on information provided by the airport	early April 2009
Negotiation meetings scheduled with the airport	early June 2009
Negotiations completed and OTA executed	late August 2009

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix S. EBSP ARRA Milestones (continued)

Project Timelines – New Facility Modification Agreement Projects (continued)

Major Milestones	Estimated Completion Date
San Francisco International Airport (SFO)	
Notification letter sent to airport	March 2009
Draft OTA sent to airport to review the terms and conditions	mid March 2009
Airports submit updated cost information to TSA	late March 2009
Cost validations updated based on information provided by the airport	late March 2009
Negotiation meetings scheduled with the airport	late April 2009
Negotiations completed and OTA executed	early June 2009
Sacramento International Airport (SMF)	
Notification letter sent to airport	March 2009
Draft OTA sent to airport to review the terms and conditions	mid March 2009
Airports submit updated cost information to TSA	early April 2009
Cost validations updated based on information provided by the airport	mid April 2009
Negotiation meetings scheduled with the airport	late May 2009
Negotiations completed and OTA executed	August 2009
Jackson Hole Airport (JAC)	
Notification letter sent to airport	March 2009
Draft OTA sent to airport to review the terms and conditions	mid March 2009
Airports submit updated cost information to TSA	late March 2009
Cost validations updated based on information provided by the airport	mid April 2009
Negotiation meetings scheduled with the airport	late April 2009
Negotiations completed and OTA executed	mid June 2009

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix S. EBSP ARRA Milestones (continued)

Major Milestones	Estimated Completion Date
Huntsville International -- Carl T. Jones Field Airport (HSV)	
Notification letter sent to airport	March 2009
Draft OTA sent to airport to review the terms and conditions	mid March 2009
Airports submit updated cost information to TSA	early April 2009
Cost validations updated based on information provided by the airport	mid April 2009
Negotiation meetings scheduled with the airport	early September 2009
Negotiations completed and OTA executed	late September 2009
Orlando International Airport (MCO) -- East Terminal	
Notification letter sent to airport	March 2009
Draft OTA sent to airport to review the terms and conditions	mid March 2009
Airports submit updated cost information to TSA	early April 2009
Cost validations updated based on information provided by the airport	mid May 2009
Negotiation meetings scheduled with the airport	early June 2009
Negotiations completed and OTA executed	late July 2009
Orlando International Airport (MCO) -- Disney Terminal	
Notification letter sent to airport	March 2009
Draft OTA sent to airport to review the terms and conditions	mid March 2009
Airports submit updated cost information to TSA	early April 2009
Cost validations updated based on information provided by the airport	mid April 2009
Negotiation meetings scheduled with the airport	early September 2009
Negotiations completed and OTA executed	late September 2009

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix S. EBSP ARRA Milestones (continued)

Project Timelines – New Facility Modification Agreement Projects (continued)

Major Milestones	Estimated Completion Date
James M. Cox Dayton International Airport (DAY)	
Notification letter sent to airport	March 2009
Draft OTA sent to airport to review the terms and conditions	mid March 2009
Airports submit updated cost information to TSA	late April 2009
Cost validations updated based on information provided by the airport	late April 2009
Negotiation meetings scheduled with the airport	late July 2009
Negotiations completed and OTA executed	late August 2009
Port Columbus International (CMH)	
Notification letter sent to airport	March 2009
Draft OTA sent to airport to review the terms and conditions	mid March 2009
Airports submit updated cost information to TSA	late March 2009
Cost validations updated based on information provided by the airport	early April 2009
Negotiation meetings scheduled with the airport	early July 2009
Negotiations completed and OTA executed	late September 2009
Hartsfield – Jackson Atlanta International Airport (ATL)	
Notification letter sent to airport	March 2009
Draft OTA sent to airport to review the terms and conditions	mid March 2009
Airports submit updated cost information to TSA	late March 2009
Cost validations updated based on information provided by the airport	early April 2009
Negotiation meetings scheduled with the airport	early July 2009
Negotiations completed and OTA executed	late September 2009

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix S. EBSP ARRA Milestones (continued)

Project Timelines – New Facility Modification Agreement Projects (continued)

Major Milestones	Estimated Completion Date
Louis Armstrong New Orleans International Airport (MSY)	
Notification letter sent to airport	March 2009
Draft OTA sent to airport to review the terms and conditions	mid March 2009
Airports submit updated cost information to TSA	early April 2009
Cost validations updated based on information provided by the airport	mid May 2009
Negotiation meetings scheduled with the airport	early October 2009
Negotiations completed and OTA executed	March 2009
Lambert-Saint Louis International Airport (STL)	
Notification letter sent to airport	July 2009
Draft OTA sent to airport to review the terms and conditions	July 2009
Airports submit updated cost information to TSA	late July 2009
Cost validations updated based on information provided by the airport	mid August 2009
Negotiation meetings scheduled with the airport	late August 2009
Negotiations completed and OTA executed	late September 2009
Washington Dulles International Airport (IAD)	
Notification letter sent to airport	July 2009
Draft OTA sent to airport to review the terms and conditions	July 2009
Airports submit updated cost information to TSA	late July 2009
Cost validations updated based on information provided by the airport	mid August 2009
Negotiation meetings scheduled with the airport	late August 2009
Negotiations completed and OTA executed	late September 2009

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix S. EBSP ARRA Milestones (continued)

Project Timelines – New Facility Modification Agreement Projects (continued)

Major Milestones	Estimated Completion Date
Yellowstone Regional Airport (COD)	
Notification letter sent to airport	July 2009
Draft OTA sent to airport to review the terms and conditions	July 2009
Airports submit updated cost information to TSA	late July 2009
Cost validations updated based on information provided by the airport	mid August 2009
Negotiation meetings scheduled with the airport	late August 2009
Negotiations completed and OTA executed	late September 2009
William P. Hobby Airport (HOU)	
Notification letter sent to airport	July 2009
Draft OTA sent to airport to review the terms and conditions	July 2009
Airports submit updated cost information to TSA	late July 2009
Cost validations updated based on information provided by the airport	mid August 2009
Negotiation meetings scheduled with the airport	late August 2009
Negotiations completed and OTA executed	late September 2009
St. Petersburg-Clearwater International Airport (PIE)	
Notification letter sent to airport	July 2009
Draft OTA sent to airport to review the terms and conditions	July 2009
Airports submit updated cost information to TSA	late July 2009
Cost validations updated based on information provided by the airport	mid August 2009
Negotiation meetings scheduled with the airport	early September 2009
Negotiations completed and OTA executed	late October 2009

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix S. EBSP ARRA Milestones (continued)

Project Timelines – New Facility Modification Agreement Projects (continued)

Major Milestones	Estimated Completion Date
Gallatin Field Airport (BZN)	
Notification letter sent to airport	July 2009
Draft OTA sent to airport to review the terms and conditions	July 2009
Airports submit updated cost information to TSA	late July 2009
Cost validations updated based on information provided by the airport	mid August 2009
Negotiation meetings scheduled with the airport	early September 2009
Negotiations completed and OTA executed	late December 2009
Tulsa International Airport (TUL)	
Notification letter sent to airport	July 2009
Draft OTA sent to airport to review the terms and conditions	July 2009
Airports submit updated cost information to TSA	late July 2009
Cost validations updated based on information provided by the airport	mid August 2009
Negotiation meetings scheduled with the airport	late September 2009
Negotiations completed and OTA executed	late December 2009
Charlotte/Douglas International Airport (CLT)	
Notification letter sent to airport	July 2009
Draft OTA sent to airport to review the terms and conditions	July 2009
Airports submit updated cost information to TSA	late July 2009
Cost validations updated based on information provided by the airport	mid August 2009
Negotiation meetings scheduled with the airport	mid October 2009
Negotiations completed and OTA executed	January 2010

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix S. EBSP ARRA Milestones (continued)

Project Timelines – New Facility Modification Agreement Projects (continued)

Major Milestones	Estimated Completion Date
Colorado Springs Airport (COS)	
Notification letter sent to airport	July 2009
Draft OTA sent to airport to review the terms and conditions	July 2009
Airports submit updated cost information to TSA	late July 2009
Cost validations updated based on information provided by the airport	mid August 2009
Negotiation meetings scheduled with the airport	mid October 2009
Negotiations completed and OTA executed	January 2010
Little Rock National Airport (LIT)	
Notification letter sent to airport	July 2009
Draft OTA sent to airport to review the terms and conditions	July 2009
Airports submit updated cost information to TSA	late July 2009
Cost validations updated based on information provided by the airport	mid August 2009
Negotiation meetings scheduled with the airport	mid September 2009
Negotiations completed and OTA executed	November 2009
San Antonio International (SAT)	
Notification letter sent to airport	February 10, 2009
Draft OTA sent to airport to review the terms and conditions	March 22, 2009
Airports submit updated cost information to TSA	April 10, 2009
Cost validations updated based on information provided by the airport	April 17, 2009
Negotiation meetings scheduled with the airport	late May 2009
Negotiations completed and OTA executed	September 2009

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY



Checkpoint Support Expenditure Plan

Fiscal Year 2009 Report to Congress

1st and 2nd Quarter Update

August 26, 2009



Homeland
Security

Transportation Security Administration

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Message from the Acting Administrator of the Transportation Security Administration

August 26, 2009

I am pleased to present the following report, "Checkpoint Support Expenditure Plan," which has been prepared by the Transportation Security Administration.

This document has been compiled in response to requirements in the Fiscal Year 2009 Department of Homeland Security Appropriations Act (P.L. 110-329) and the accompanying Explanatory Statement and Senate Report 110-396. It provides an expenditure plan update for the procurement and installation of emerging technologies and advanced threat detection systems for airport passenger checkpoints.

Pursuant to Congressional requirements, this report is being provided to the following Members of Congress:

The Honorable David E. Price
Chairman, House Appropriations Subcommittee on Homeland Security

The Honorable Harold Rogers
Ranking Member, House Appropriations Subcommittee on Homeland Security

The Honorable Robert C. Byrd
Chairman, Senate Appropriations Subcommittee on Homeland Security

The Honorable George V. Voinovich
Ranking Member, Senate Appropriations Subcommittee on Homeland Security

If I may be of further assistance, please do not hesitate to contact me at (571) 227-2845 or the Department's Acting Chief Financial Officer, Peggy Sherry, at (202) 447-5751.

Sincerely yours,



Gale D. Rossides
Acting Administrator

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Executive Summary

The Fiscal Year (FY) 2009 Department of Homeland Security Appropriations Act (P.L. 110-329) and the accompanying Explanatory Statement and Senate Report 110-396 require the Department to provide a quarterly expenditure plan update for Checkpoint Support and include information on specific technologies for purchase, project timelines, a schedule for obligation and a table detailing actual versus anticipated unobligated balances at the close of the fiscal year.

The Checkpoint Support funding is implemented through the Passenger Screening Program. This report includes the 1st and 2nd quarter updates to the FY 2009 Spend Plan.

Checkpoint Support - \$250 Million

PSP tests, procures, deploys, integrates and provides life cycle support for security equipment to screen passengers and carry-on baggage at passenger checkpoint lanes at domestic airports. PSP is responsible for technologies that screen over 700,000,000 passengers per year at approximately 450 of the Nation's airports.

To simplify funds management, it was necessary to reallocate some of the FY 2009 funding to accommodate changes in usage of the prior year's carryovers. FY 2009 and prior procurement quantities changed for Whole Body Imagers, Advanced Technology and Credential Authentication Technology.

These reallocations had no effect on the total quantity to be procured by the fiscal year's end.

Advanced Surveillance Program (ASP) utilizes the existing infrastructure owned and operated by the transportation authority for remote monitoring, threat detection and assessment in a partnership agreement to provide enhanced situational awareness.

ASP will reallocate funding from Phoenix (PHX) of \$1.0 million and Atlanta (ATL) of \$0.1 million, as PHX and ATL reduced scope eliminating the need for checkpoint cameras at this time.

- \$0.8 million will be reallocated to Chicago in order to complete surveillance installation at their checkpoints;
- \$0.1 million will be reallocated to Cleveland to add networking capability;
- \$0.1 million will be reallocated to Louis Munoz Marin International Airport to complete surveillance installation;
- \$0.1 million will be reallocated to Philadelphia for complete surveillance installation.

The Third Quarter report will include ARRA funding.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.



Checkpoint Support Expenditure Plan 1st and 2nd Quarter Update

Table of Contents

I.	Legislative Requirement	1
II.	Background.....	2
III.	Expenditure Plan.....	4
	Program Initiatives.....	5
	Description of Initiative I – Advanced Technology X-Ray	5
	Description of Initiative II – Universal Conveyor Systems (UCS)	5
	Description of Initiative III – Whole Body Imager	6
	Description of Initiative IV – Credential Authentication Technology	6
	Description of Initiative V – Bottled Liquids Scanner	7
	Description of Initiative VI – Next Generation Explosives Trace Detector (ETD)	7
	Description of Initiative VII – Integration.....	8
	Description of Initiative VIII – Program Operations and Management	8
	Description of Initiative IX – Technical and Engineering Initiatives.....	8
	Description of Initiative X – Safety and Optimization	9
	Description of Initiative XI – Checkpoint Reconfiguration	9
	Description of Initiative XII – Advanced Surveillance Program (ASP).....	10
	Description of Initiative XIII – Personnel Compensation and Benefits(PC&B).....	10
IV.	Appendices.....	11
	Appendix A: Costs by Airport	12
	Appendix B: Abbreviations/Acronyms.....	12
	Appendix C: PSP FY 2009 Summary Spend Plan.....	17
	Appendix D: PSP Obligation Data	19
	Appendix E: PSP Milestones	20
	Appendix F: Actual vs. Anticipated Unobligated Balance	21

FOR OFFICIAL USE ONLY

I. Legislative Requirement

This report is provided in compliance with requirements in the Fiscal Year (FY) 2009 Department of Homeland Security Appropriations Act (P.L. 110-329) and the accompanying Explanatory Statement and Senate Report 110-396, which include the following language.

P.L. 110-329 includes the following provisions:

EXPLOSIVES DETECTION SYSTEMS

As discussed in the Senate report, TSA shall provide quarterly updates on EDS and checkpoint expenditures, on an airport-by-airport basis. These updates shall include information on the specific technologies for purchase, project timelines, a schedule for obligation, and a table detailing actual versus anticipated unobligated balances at the close of the fiscal year, with an explanation of any deviation from the original plan.

The Explanatory Statement offers the following guidance:

As discussed in the Senate report, TSA shall provide quarterly updates on EDS and checkpoint expenditures, on an airport-by-airport basis. These updates shall include information on the specific technologies for purchase, project timelines, a schedule for obligation, and a table detailing actual versus anticipated unobligated balances at the close of the fiscal year, with an explanation of any deviation from the original plan.

In addition, Senate Report 110-396 includes the following:

EXPENDITURE PLANS FOR EDS/CHECKPOINT TECHNOLOGIES

Additionally, the Committee includes a new requirement for the expenditure plans to be updated quarterly and to include the following new information: specific technologies planned for purchase; project timelines; a schedule for obligation; and a table detailing actual unobligated balances versus anticipated unobligated balances at the close of the fiscal year. The quarterly updates shall also include an explanation for any deviation from the original plan.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

II. Background

Mission

The Passenger Screening Program's (PSP's) Mission Need supports prevention and protection from terrorist and criminal actions in the aviation transportation environment. PSP specifically focuses on technology and processes utilized in and near the passenger screening checkpoint in order to focus on the air travel passenger security mission, which includes:

The PSP mission: PSP is responsible for the acquisition of technology that identifies threats concealed on people and their carry-on items entering the sterile area of the airport terminal through the passenger screening checkpoint. The checkpoint is defined as the screening equipment, processes and operating personnel collectively required to perform the security mission.

Purpose

PSP accomplishes its mission by identifying, testing, procuring, deploying, integrating and sustaining equipment that identifies threats concealed on passengers and their carry-on items as they enter the airport terminal through the passenger screening checkpoint.

Goals

PSP supports Goal One of the DHS Strategic Plan, FYs 2008–2013, “Protect Our Nation from Dangerous People.”

PSP Objectives:

- **Explosive Detection:** Detect explosive threats, weapons and other prohibited items concealed on passengers and their carry-on items
- **Screening Efficiency:** Improve checkpoint efficiency through process automation
- **Layered Security:** Enable layered, integrated security solution

Accomplishments

The following are accomplishments of PSP technologies:

Advanced Technology X-Ray (AT)

- Over 650 AT (first generation) operational units deployed nationwide have expanded the capabilities of the Transportation Security Officers (TSOs) at the checkpoint by replacing legacy Threat Image Projection (TIP) Ready X-Ray (TRX) systems. Advanced Technology (AT) systems are penetration x-ray based technologies that provide an enhanced view of a bag's contents through improved image resolution. Also, an added

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid “need-to-know” without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

dimension to the displayed image provides better material discrimination for TSOs to discern each object inside a bag. AT systems are upgradeable, offering a cost-effective platform to develop enhanced detection capabilities. Additionally, AT systems can include the universal conveyor system (UCS), which diverts bags requiring a secondary search. The UCS will assist in maintaining positive control and tracking of all passenger carry-on baggage until a clear indication of status regarding the baggage is provided by the screening technology and a decision is made by TSOs to deliver the baggage to the passenger. This functionality will improve overall throughput and minimize congestion on the exit side of the AT system. Deployments are ongoing and the second generation of AT will undergo testing in the spring/summer 2009 timeframe.

Whole Body Imager (WBI)

- The Whole Body Imager (WBI) is a new imaging capability that will be used to inspect a passenger for concealed weapons (metal and non-metal), explosives and other prohibited items. In addition, the WBI offers operators the opportunity to review anomalies on an individual, to determine if a hand wand and/or physical pat-down inspection is required. WBIs could ultimately be the primary passenger screening technology in lieu of using an Enhanced Metal Detector (EMD). TSA has assessed two types of technologies for the WBIs, including X-ray backscatter and millimeter wave technology. Both offer safe and effective whole body screening for weapons and explosives concealed on a person. Deployments are ongoing and the second generation of WBI will undergo testing in the Spring/Summer 2009 timeframe.

Bottled Liquid Scanner

- The Bottled Liquids Scanner is a detection capability that can discriminate explosives or flammable liquids from common, benign liquids carried by passengers. The devices analyze substances within a container (bottle or can), measuring particular characteristics of the contents and distinguishing between benign and hazardous liquids in a matter of seconds. The second generation devices perform scans without breaking seals or contaminating passengers' property and will greatly reduce annual consumable costs.

The following chart shows enacted amounts since inception of the Checkpoint Support Program, Project, and Activity (PPA). Values are in millions of dollars.

2002	2003	2004	2005	2006	2007	07 Supp	2008	2009	ARRA	TOTAL
\$ 38.00	\$ 40.00	\$ 61.86	\$ 123.50	\$ 164.00	\$ 173.37	\$ 25.00	\$ 250.00	\$ 250.00	\$ 300.00	\$ 1,425.73

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

III. Expenditure Plan

Summary of PSP Expenditure Plan (in \$ Million)

Section	Initial	Revised*
Technology	\$144.5	\$149.7
Program Operations and Management	\$40.9	\$35.7
Technical and Engineering Initiatives	\$22.6	\$22.6
Safety and Optimization	\$13.5	\$13.5
Checkpoint Reconfiguration	\$11.5	\$11.5
Advanced Surveillance Program	\$11.0	\$11.0
Personnel Compensation and Benefits	\$6.0	\$6.0
Total	\$250.0	\$250.0

*Reallocations were necessary to account for carryover funds used to procure services that would have normally been procured with FY 2009 funding.

Technology Purchases and Percentages to Reach Full Operating Capability (FOC)

Technology	FOC	Purchases with Prior Year Funds	Purchases with FY 2009 Funds	TOTAL
Advanced Technology *	2,325	1,009	436	1,445
Universal Conveyor Systems	2,325	0	200	200
Whole Body Imagers*	878	47	175	222
Credential Authentication Technology*	878	112	288	400
Bottled Liquids Scanners	1,300	600	200	800
Explosives Trace Detectors	1,500	100	100	200

*Equipment quantities to be purchased with FY 2009 funds and carryover funds were reallocated for Whole Body Imagers, Advanced Technology and Credential Authentication Technology. However, the total quantity to be procured by the FY's end is unchanged.

Technology	FOC	Prior Year	FY 2009	TOTAL Percentage of FOC
Advanced Technology	2,325	43%	62%	62%
Universal Conveyor Systems	2,325	0%	9%	9%
Whole Body Imagers	878	5%	25%	25%
Credential Authentication Technology	878	12%	45%	45%
Bottled Liquids Scanners	1,300	46%	62%	62%
Explosives Traces Detectors	1,500	7%	13%	13%

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Program Initiatives

Description of Initiative I - Advanced Technology X-Ray

- AT systems are penetration x-ray-based technologies that provide an enhanced view of a bag's contents through improved image resolution beyond the capabilities of the currently fielded TRX equipment. Also, an added dimension to the displayed image provides better material discrimination for TSO to discern each object inside a bag. AT offers a cost-effective platform to develop enhanced detection capabilities. Future enhancements may include an enhanced conveyor system. The first generation of AT is currently being deployed with over 650 units installed at airports nationwide. The second generation of AT with upgraded capability and functionality is currently in the development stage.
- Obligations to date: \$103.7 million
- Projected FY 2009 obligations: FY 2009 - \$54.5 million
- Projected FY 2009 expenditures by year: FY 2010 - \$54.5 million
- Major performance objectives:
 - Probability of detection of threat items: Classified
 - Throughput: ≥ 440 bags per hour with operator intervention
 - Operational availability: $\geq 98\%$
- Activities and milestones/accomplishments:
 - Initial Operational Capability (IOC): Third Quarter FY 2008
 - Qualification Testing and Evaluation (QT&E): Second Quarter FY 2009
 - Operational Testing and Evaluation (OT&E): Third Quarter FY 2009
 - Contract award: Fourth Quarter FY 2009
 - FOC: With FY 2009 funds, Fourth Quarter FY 2010 accelerated from Second Quarter FY 2014

Description of Initiative II - Universal Conveyor Systems (UCS)

- UCS are carry-on baggage handling conveyor systems added on to the AT systems to support automated diversion of alarm bags from the cleared baggage stream.
- Obligations to date: \$0.0 million
- Projected FY 2009 obligations: FY 2009 - \$25.0 million
- Projected FY 2009 expenditures by year: FY 2010 - \$25.0 million
- Activities and milestones/accomplishments:
 - Contract award: Fourth Quarter FY 2009
 - IOC: Fourth Quarter FY 2009

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Description of Initiative III - Whole Body Imager (WBI)

- WBIs provide an imaging capability used to inspect a passenger's body for concealed weapons (metal and nonmetal), explosives and other prohibited items in place of a metal detection wand inspection and physical pat-down. The WBI could potentially become a primary screening technology, which either could be used in conjunction with an Enhanced Metal Detector (EMD) or in lieu of an EMD.
- Obligations to date: \$12.0 million
- Projected FY 2009 obligations: FY 2009 - \$28.9 million
- Projected FY 2009 expenditures by year: FY 2010 - \$28.9 million
- Major performance objectives:
 - Probability of threat detection: Classified
 - Throughput: ≥ 200 passengers per hour
 - Operational availability: $\geq 98\%$
- Activities and milestones/accomplishments:
 - QT&E: Second Quarter FY 2009
 - OT&E: Third Quarter FY 2009
 - Contract award: Fourth Quarter FY 2009
 - IOC: Fourth Quarter FY 2009
 - FOC: Fourth Quarter FY 2014

Description of Initiative IV – Credential Authentication Technology

- Systems provide a primary means for automated credential authentication of passenger travel documents and forms of identification that are presented to TSOs by passengers during the security checkpoint screening process, as well as those forms of identification presented by airport and airline personnel to access sterile areas. This system will increase TSOs' abilities to locate fraudulent IDs and validate the issuing authority and authenticity of boarding passes at security checkpoints.
- Obligations to date: \$0.0 million
- Projected FY 2009 obligations: FY 2009 - \$6.5 million
- Projected FY 2009 expenditures by year: FY 2010 - \$6.5 million
- Activities and milestones/accomplishments:
 - RFP: Second Quarter FY 2009
 - Contract Award: Fourth Quarter FY 2009
 - FOC: Second Quarter FY 2011

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Description of Initiative V - Bottled Liquids Scanner

- BLS are explosive detection systems that differentiate liquid explosives from common, benign liquids. BLS utilize a variety of technologies to detect liquid explosives and explosive precursors, including vapor detection, X-ray detection, detection using the dielectric properties of the materials being scanned or optical detection using Raman spectroscopy.
- Obligations to date: \$0.0 million
- Projected FY 2009 obligations: FY 2009 - \$7.5 million
- Projected FY 2009 expenditures by year: FY 2010 - \$7.5 million
- Major performance objectives:
 - Probability of Detection of Threat Items: Classified
 - Throughput: ≥ 180 samples per hour
 - Operational Availability: $\geq 98\%$
- Activities and milestones/accomplishments:
 - IOC: TBD: Delayed from Fourth Quarter FY 2008
 - QT&E: Second Quarter FY 2009
 - OT&E: Second Quarter FY2009
 - Contract Award: Fourth Quarter FY 2009
 - FOC: Second Quarter FY 2011

Description of Initiative VI - Next Generation Explosives Trace Detector (ETD)

- NextGen ETD identifies a larger range of explosives than earlier models. The NextGen ETDs have enhanced explosives detection capability, including increased sensitivity and the ability to detect new threats. The mean time to repair will be significantly less than the current ETD. In addition, the NextGen ETDs will have a Field Data Reporting System and will be Security Technology Integration Program capable. Because of these significant improvements, a lower lifecycle cost is expected.
- Obligations to date: \$6.1 million
- Projected FY 2009 obligations: FY 2009 - \$6.0 million
- Projected FY 2009 expenditures by year: FY 2010 - \$6.0 million
- Major performance objectives:
 - Probability of Detection of Threat Items: Classified
 - Throughput: 180 samples per hour, to include machine processing and analysis, when no alarms are present.
 - Operational Availability: $\geq 98\%$
- Activities and Milestones/Accomplishments:
 - QT&E: First Quarter FY 2008
 - OT&E: Second Quarter FY 2008
 - Contract award: Fourth Quarter FY 2008
 - IOC: First Quarter FY 2009
 - FOC: Fourth Quarter FY 2014

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Description of Initiative VII - Integration

Relates to all tasks associated with the installation of security technology equipment at geographically dispersed airports nationwide:

- Integration services can include moving equipment, small scale facility modification, or electrical and plumbing.
- Projected FY 2009 obligations: FY 2009 - \$21.3 million
- Projected FY 2009 expenditures by year: FY 2009 - \$15.0 million; FY 2010 - \$6.3 million

Description of Initiative VIII - Program Operations and Management

Program Operations and Management encompasses activities needed for the procurement and deployment of security systems to the Nation's airports. The following activities make up this initiative:

- **Project Logistics** operation activities deal with the procurement, distribution and replacement of systems to and from the field.
- **Technical Engineering** activities encompass requirements review, technical representation and technical management support.
- **Independent Verification and Validation** activities encompass factory acceptance testing, site acceptance testing and integrated site testing.
- **Installation and Design Services** activities encompass architectural design and review, site survey and construction package review.
- **Data Collection** activities are those associated with documentation, reports and technical support of testing.
- **TSA Systems Integration Facility** provides an operationally-realistic environment to evaluate current/new advanced screening technologies, processes and procedures against known threats to transportation venues, particularly air transportation venues.
- **Program Resource and Data Management** activities encompass project management support, financial management and analysis, data management and project scheduling.
- Projected FY 2009 obligations: FY 2009 - \$35.7 million
- Projected FY 2009 expenditures by year: FY 2009 - \$20.0 million; FY 2010 - \$15.7 million

Description of Initiative IX - Technical and Engineering Initiatives

- **Security Technology Integration Program** is an agency-wide system that enables TSA to connect all Transportation Security Equipment (TSE) to one data management system that will facilitate the exchange of information across the network and facilitate maintenance servicing and diagnostic information.
- **Operational Integration of Emerging Technology** conducts data collection, research, and field tests to verify systems, operational innovations and screening upgrades work in a variety of conditions, climates and processes. Reliability, maintainability and availability will be assessed on new technologies and innovations to effectively make

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

decisions concerning their deployability and usefulness. Examples of emerging technologies to be field tested and piloted include WBI, AT, BLS and CAT (including wait time collection pilot).

- **Threat Image Projection (TIP)** keeps Transportation Security Officers alert and exposes them to a variety of prohibited item images they may not normally see. It is also used as an evaluation tool to assess the visual inspection performance of detecting prohibited items by a TSO during real working hours instead of in-lab conditions. **Engineering Changes** are required to modify technology to support enhanced capabilities such as throughput, detection, operator interface, etc.
- **Exit Lane Breach Control** project is to test and evaluate the performance capabilities and technical viability of technologies that minimize the risk of unauthorized access and reduce resource requirements at exit lanes.
- Projected FY 2009 obligations: FY 2009 - \$22.6 million
- Projected FY 2009 expenditures by year: FY 2009 - \$15.0 million; FY 2010 - \$7.6 million

Description of Initiative X – Safety and Optimization

- The Safety and Optimization Program improves the safety and efficiency of checkpoints and checked baggage screening operations by deploying ancillary equipment and enhancing the design and layout of screening areas.
- Funding will be used to procure equipment and services to complete airport safety enhancement projects to minimize the amount of TSOs injured on the job.
- Projected FY 2009 obligations: FY 2009 - \$13.5 million
- Projected FY 2009 expenditures by year: FY 2009 - \$9.0M; FY 2010 - \$4.5 million

Description of Initiative XI – Checkpoint Reconfiguration

- Checkpoint Reconfigurations are required at airports to maintain or improve throughput due to the growth in passenger traffic and the evolution of the airline industry. Reconfiguration of checkpoints can also be required as emerging technologies are deployed in order to efficiently utilize the checkpoint space.
- Funding will be used to procure glass for wand stations, adjustable divest and composure tables, ancillary equipment for checkpoints such as podiums and benches, as well as reconfiguration of checkpoint equipment and layouts to accommodate emerging technologies and redesign to make checkpoints more efficient.
- Projected FY 2009 obligations: FY 2009 - \$11.0 million
- Projected FY 2009 expenditures by year: FY 2010 - \$11.0 million

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Description of Initiative XII - Advanced Surveillance Program (ASP)

- ASP utilizes the existing infrastructure owned and operated by the transportation authority for remote monitoring, threat detection and assessment in a partnership agreement to provide enhanced situational awareness of the checkpoint and checked baggage area of airports.
- Projected FY 2009 obligations: FY 2009 - \$11.0 million
- Projected FY 2009 expenditures by year: FY 2010 - \$11.0 million
- Activities and Milestones/Accomplishments:
 - Site Visits: TBD by airport
 - Proposals: Third Quarter FY 2009
 - Contract Awards: Third Quarter FY 2009
- Changes to original spend plan
 - Reduce PHX by \$1 million
 - Reduce ATL by \$0.1 million
 - Increase PHL by \$0.1 million
 - Add ORD \$0.8 million to complete surveillance installations at their checkpoints
 - Add CLE \$0.1 million to add networking capability
 - Add SJU \$0.1 million to complete surveillance installation

Description of Initiative XIII – Personnel Compensation and Benefits (PC&B)

- Projected FY 2009 obligations: FY 2009 - \$6.0 million
- Projected FY 2009 expenditures by year: FY 2009 - \$6.0 million

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

IV. Appendices

- A. Costs by Airport
- B. Abbreviations/Acronyms
- C. PSP FY 2009 Summary Spend Plan
- D. PSP Obligation Data
- E. PSP Milestones
- F. Actual vs. Anticipated Unobligated Balance

FOR OFFICIAL USE ONLY

Appendix A: Costs by Airport

Airport	SIZE	Planned ETD	Actual ETD	Planned AT	Actual AT	Planned UCS	Actual UCS	Planned WBI	Actual WBI	Planned BLS	Actual BLS	Planned SOD	Actual SOD	Planned CAT	Actual CAT
JFK	X	22		10	29					23				35	
LAX	X	14			3	34				29					
DCA	X	3							2	6					
BWI	X	8			1					8		2		14	
IAD	X	4			4					9					
ORD	X	13		51	51			2		19		2			
MIA	X	6			13					10					
LGA	X	3		9	9					9					
EWB	X	15		12	1			3		12					
IAH	X	12		11	11					11		1			
BOS	X	9		16	13			6		16		2			
PHL	X	2		14	21					9					
DTW	X	19		34	18					12					
DFW	X	13			8					22					
ATL	X	15			18				3	11		2			
SFO	X	12		14	10				1	14					
MSP	X	9		10	10					10					
MCO	X	3		10	9					10					
HNL	X	9		9	9					9					
DEN	X	4								7					
SJU	X	8		6	4					6					
LAS	X	1				2				12					
SEA	X	7		9	10	6				9		2			
CLT	X	3		5	4					5					
SAN	I	4		8	7					8					
PHX	X	7			1					11					
FLL	X	13		9	9					9					
GUM	I			5						1					
CVG	X	4		5	4					6					
RDU	I	1		5	5					5					

Planned Tech Cost	Actual Tech Cost ¹	Planned Set Up Cost	Actual Set Up Cost ¹
\$ 4,220,000	\$ 1,902,110	\$ 572,089	\$ 874,582
\$ 6,177,500	\$ 196,770	\$ 1,076,629	\$ 90,474
\$ 405,000	\$ 308,394	\$ 25,098	\$ 90,642
\$ 1,405,000	\$ 172,238	\$ 147,864	\$ 30,158
\$ 577,500	\$ 688,952	\$ 35,597	\$ 120,632
\$ 8,499,500	\$ 3,345,090	\$ 1,768,027	\$ 1,538,058
\$ 735,000	\$ 2,239,094	\$ 45,930	\$ 392,054
\$ 1,642,500	\$ 1,550,142	\$ 302,919	\$ 271,422
\$ 3,333,000	\$ 65,590	\$ 584,955	\$ 30,158
\$ 2,662,500	\$ 721,490	\$ 427,151	\$ 331,738
\$ 4,416,000	\$ 2,239,094	\$ 870,982	\$ 392,054
\$ 2,207,500	\$ 1,377,390	\$ 449,609	\$ 633,318
\$ 5,840,000	\$ 3,100,284	\$ 1,128,868	\$ 542,844
\$ 1,605,000	\$ 1,377,904	\$ 100,226	\$ 241,264
\$ 1,622,500	\$ 1,643,211	\$ 130,463	\$ 678,807
\$ 2,995,000	\$ 1,876,577	\$ 501,274	\$ 346,901
\$ 2,165,000	\$ 655,900	\$ 359,810	\$ 301,580
\$ 1,805,000	\$ 1,550,142	\$ 335,210	\$ 271,422
\$ 2,002,500	\$ 1,550,142	\$ 327,519	\$ 271,422
\$ 502,500	\$ -	\$ 31,331	\$ -
\$ 1,455,000	\$ 262,360	\$ 226,546	\$ 120,632
\$ 760,000	\$ -	\$ 86,012	\$ -
\$ 2,942,500	\$ 655,900	\$ 533,767	\$ 301,580
\$ 992,500	\$ 262,360	\$ 173,755	\$ 120,632
\$ 1,540,000	\$ 459,130	\$ 274,728	\$ 211,106
\$ 832,500	\$ 65,590	\$ 52,163	\$ 30,158
\$ 2,242,500	\$ 590,310	\$ 343,919	\$ 271,422
\$ 662,500	\$ -	\$ 152,923	\$ -
\$ 1,090,000	\$ 688,952	\$ 179,988	\$ 120,632
\$ 872,500	\$ 327,950	\$ 165,555	\$ 150,790

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Costs by Airport (Continued)

Airport	SIZE	Planned ETD	Actual ETD	Planned AT	Actual AT	Planned UCS	Actual UCS	Planned WBI	Actual WBI	Planned BLS	Actual BLS	Planned SOD	Actual SOD	Planned CAT	Actual CAT
PDX	I	3		6	5					6					
MEM	I	4		4						5					
STL	X	3		6	5					6					
JAX	I	4		2	2				1	2					
ANC	I			3	3					3					
SYR	II			3						3					
SJC	I	2		6	2					6					
SLC	I			6	5				1	6		2			
BUF	I			2	3					2					
BNA	I	5		4						4					
SAT	I	4		3	3					3					
PIT	I			4	4					4					
IND	IV				1	14				5		2			
GSN	II			2	3					1					
TPA	I	1		7	6				2	7					
PBI	I	1		4						4					
ONT	I	1		2						2					
MKE	I	2		4	4					4					
MDW	I			5	5										
MCI	I	1		10	11										
HOU	I			6											
DAL	I	1		2	3										
CLE	I	4		5	4										
BUR	I	1		2	2										
BHM	I			2											
BDL	I			3	3										
TUS	I	1		6	2										
SNA	I	1		4	4										
SFB	II	1		3	2										
PVD	I	2		2	2										

Planned Tech Cost	Actual Tech Cost ¹	Planned Set Up Cost	Actual Set Up Cost ¹
\$ 1,155,000	\$ 861,190	\$ 206,046	\$ 150,790
\$ 927,500	\$ -	\$ 147,697	\$ -
\$ 1,155,000	\$ 327,950	\$ 206,046	\$ 150,790
\$ 565,000	\$ 498,673	\$ 80,982	\$ 105,637
\$ 487,500	\$ 196,770	\$ 96,873	\$ 90,474
\$ 487,500	\$ -	\$ 96,873	\$ -
\$ 1,095,000	\$ 344,476	\$ 201,946	\$ 60,316
\$ 1,285,000	\$ 1,015,387	\$ 239,246	\$ 196,111
\$ 325,000	\$ 516,714	\$ 64,582	\$ 90,474
\$ 950,000	\$ -	\$ 149,664	\$ -
\$ 727,500	\$ 196,770	\$ 113,273	\$ 90,474
\$ 650,000	\$ 262,360	\$ 129,164	\$ 120,632
\$ 2,247,500	\$ 65,590	\$ 450,377	\$ 30,158
\$ 287,500	\$ 196,770	\$ 62,449	\$ 90,474
\$ 1,197,500	\$ 1,341,822	\$ 230,137	\$ 271,590
\$ 710,000	\$ -	\$ 133,264	\$ -
\$ 385,000	\$ -	\$ 68,682	\$ -
\$ 770,000	\$ 688,952	\$ 137,364	\$ 120,632
\$ 625,000	\$ 861,190	\$ 150,790	\$ 150,790
\$ 1,310,000	\$ 1,894,618	\$ 305,680	\$ 331,738
\$ 750,000	\$ -	\$ 180,948	\$ -
\$ 310,000	\$ 516,714	\$ 64,416	\$ 90,474
\$ 865,000	\$ 688,952	\$ 167,190	\$ 120,632
\$ 310,000	\$ 344,476	\$ 64,416	\$ 60,316
\$ 250,000	\$ -	\$ 60,316	\$ -
\$ 375,000	\$ 516,714	\$ 90,474	\$ 90,474
\$ 810,000	\$ 131,180	\$ 185,048	\$ 60,316
\$ 560,000	\$ 262,360	\$ 124,732	\$ 120,632
\$ 435,000	\$ 344,476	\$ 94,574	\$ 60,316
\$ 370,000	\$ 344,476	\$ 68,516	\$ 60,316

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Costs by Airport (Continued)

Airport	SIZE	Planned ETD	Actual ETD	Planned AT	Actual AT	Planned UCS	Actual UCS	Planned WBI	Actual WBI	Planned BLS	Actual BLS	Planned SOD	Actual SOD	Planned CAT	Actual CAT
ORF	I	1		2	2										
MSY	I	1		4											
GEG	I			2	2										
DAY	I			6											
ROC	II			6	2										
SMF	I	1		9	5										
RSW	I	1		4											
RNO	I	2		2	1										
OMA	I			2	2										
OKC	I			2	2										
OGG	I	2		6	2										
OAK	I			4	4										
AUS	I	2		4	2										
CMH	I	1		3											
STT	II	1		6	6										
MHT	I	1		3	3										
MDT	II	1		3											
LIH	I	2		3	4										
LGB	I			2											
FAI	II			2	2										
STX	III	1		3	3										
PPG	III	4		1	1										
FAT	II			2	2										
KOA	I	1		3	4										
GRR	II			4	2										
MLB	II			2											
DAB	II			2											
HPN	II			2											
ABE	II			2	2										
RIC	I	1		6	2				1						

Planned Tech Cost	Actual Tech Cost ¹	Planned Set Up Cost	Actual Set Up Cost ¹
\$ 310,000	\$ 344,476	\$ 64,416	\$ 60,316
\$ 560,000	\$ -	\$ 124,732	\$ -
\$ 250,000	\$ 344,476	\$ 60,316	\$ 60,316
\$ 750,000	\$ -	\$ 180,948	\$ -
\$ 750,000	\$ 344,476	\$ 180,948	\$ 60,316
\$ 1,185,000	\$ 861,190	\$ 275,522	\$ 150,790
\$ 560,000	\$ -	\$ 124,732	\$ -
\$ 370,000	\$ 172,238	\$ 68,516	\$ 30,158
\$ 250,000	\$ 344,476	\$ 60,316	\$ 60,316
\$ 250,000	\$ 344,476	\$ 60,316	\$ 60,316
\$ 870,000	\$ 131,180	\$ 189,148	\$ 60,316
\$ 500,000	\$ 688,952	\$ 120,632	\$ 120,632
\$ 620,000	\$ 131,180	\$ 128,832	\$ 60,316
\$ 435,000	\$ -	\$ 94,574	\$ -
\$ 810,000	\$ 393,540	\$ 185,048	\$ 180,948
\$ 435,000	\$ 516,714	\$ 94,574	\$ 90,474
\$ 435,000	\$ -	\$ 94,574	\$ -
\$ 495,000	\$ 262,360	\$ 98,674	\$ 120,632
\$ 250,000	\$ -	\$ 60,316	\$ -
\$ 250,000	\$ 131,180	\$ 60,316	\$ 60,316
\$ 435,000	\$ 196,770	\$ 94,574	\$ 90,474
\$ 365,000	\$ 65,590	\$ 46,558	\$ 30,158
\$ 250,000	\$ 131,180	\$ 60,316	\$ 60,316
\$ 435,000	\$ 262,360	\$ 94,574	\$ 120,632
\$ 500,000	\$ 344,476	\$ 120,632	\$ 60,316
\$ 250,000	\$ -	\$ 60,316	\$ -
\$ 250,000	\$ -	\$ 60,316	\$ -
\$ 250,000	\$ -	\$ 60,316	\$ -
\$ 250,000	\$ 131,180	\$ 60,316	\$ 60,316
\$ 810,000	\$ 285,377	\$ 185,048	\$ 105,637

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Costs by Airport (Continued)

Airport	SIZE	Planned ETD	Actual ETD	Planned AT	Actual AT	Planned UCS	Actual UCS	Planned WBI	Actual WBI	Planned BLS	Actual BLS	Planned SOD	Actual SOD	Planned CAT	Actual CAT	Planned Tech Cost	Actual Tech Cost ¹	Planned Set Up Cost	Actual Set Up Cost ¹
ABQ	I	2														\$ 120,000	\$ -	\$ 8,200	\$ -
ABI	III	1														\$ 60,000	\$ -	\$ 4,100	\$ -
AMA	II	1														\$ 60,000	\$ -	\$ 4,100	\$ -
BLI	III	2														\$ 120,000	\$ -	\$ 8,200	\$ -
BMI	III	3														\$ 180,000	\$ -	\$ 12,300	\$ -
BTV	II	1														\$ 60,000	\$ -	\$ 4,100	\$ -
CEF	III	1														\$ 60,000	\$ -	\$ 4,100	\$ -
CHO	III	1														\$ 60,000	\$ -	\$ 4,100	\$ -
CID	II	1														\$ 60,000	\$ -	\$ 4,100	\$ -
ELP	I	3														\$ 180,000	\$ -	\$ 12,300	\$ -
ERI	III	1														\$ 60,000	\$ -	\$ 4,100	\$ -
GSO	I	1														\$ 60,000	\$ -	\$ 4,100	\$ -
GSP	II	1														\$ 60,000	\$ -	\$ 4,100	\$ -
ILM	II	1														\$ 60,000	\$ -	\$ 4,100	\$ -
ITO	II	1														\$ 60,000	\$ -	\$ 4,100	\$ -
IWA	III	1														\$ 60,000	\$ -	\$ 4,100	\$ -
LEX	II	2														\$ 120,000	\$ -	\$ 8,200	\$ -
LNK	III	1														\$ 60,000	\$ -	\$ 4,100	\$ -
MBS	III	1														\$ 60,000	\$ -	\$ 4,100	\$ -
MGM	III	1														\$ 60,000	\$ -	\$ 4,100	\$ -
MYR	II	1														\$ 60,000	\$ -	\$ 4,100	\$ -
PIE	II	1														\$ 60,000	\$ -	\$ 4,100	\$ -
PNS	II	1														\$ 60,000	\$ -	\$ 4,100	\$ -
PSE	III	2														\$ 120,000	\$ -	\$ 8,200	\$ -
SBN	II	1														\$ 60,000	\$ -	\$ 4,100	\$ -
SPS	III	1														\$ 60,000	\$ -	\$ 4,100	\$ -
VLD	III	1														\$ 60,000	\$ -	\$ 4,100	\$ -
UNV	IV	2														\$ 120,000	\$ -	\$ 8,200	\$ -
BPT	IV	1														\$ 60,000	\$ -	\$ 4,100	\$ -
TUL	IV	N/A		N/A		N/A		N/A	1	N/A		N/A		N/A		\$ -	\$ 154,197	\$ -	\$ 45,321
TOTAL		346	0	472	421	56	0	11	12	401	0	15	0	49	0	\$106,996,000	\$ 48,873,690	\$19,108,888	\$13,240,370

*TUL is an added airport from the initial spend plan, thus "Planned" data will be not be applicable.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

Appendix B: Abbreviations/Acronyms

Acronym	Definition
ASP	Advanced Surveillance Program
AT	Advanced Technology X-Ray
ATSA	Aviation & Transportation Security Act
BLS	Bottled Liquids Scanner
CBIS	Checked Baggage Inspection System
CLE	Cleveland Hopkins Airport
COTR	Contracting Officer's Technical Representative
DHS	Department of Homeland Security
EBSP	Electronic Baggage Screening Program
ECP	Engineering Change Proposal
EDS	Explosives Detection Systems
ETD	Explosives Trace Detection
FAA	Federal Aviation Administration
FOC	Full Operational Capability
FY	Fiscal Year
LOI	Letter of Intent
OT&E	Operational Testing and Evaluation
OTA	Other Transactional Agreement
PC&B	Personnel Compensation and Benefits
PHX	Phoenix Sky Harbor Airport
PSP	Passenger Screening Program
QT&E	Qualification Testing and Evaluation
SJU	Louis Munoz Marin International Airport
TIP	Threat Image Projection
TRX	Threat Image Projection (TIP) Ready X-ray
TSA	Transportation Security Administration
TSIF	TSA Systems Integration Facility
TSO	Transportation Security Officer
UCS	Universal Conveyor Systems
WBI	Whole Body Imager

FOR OFFICIAL USE ONLY

Appendix C: PSP FY 2009 Summary Spend Plan

Technology	Initial # of Units	Revised # of Units	Initial FY 2009 Funds	Revised FY 2009 Funds
Advanced Technology *	508	436	\$63.5	\$54.5
Universal Conveyor Systems	200	200	\$25.0	\$25.0
Whole Body Imagers *	76	175	\$ 12.2	\$28.9
Credential Authentication Technology *	400	288	\$ 9.0	\$6.5
Bottled Liquids Scanners	200	200	\$ 7.5	\$7.5
Explosives Trace Detectors	100	100	\$6.0	\$6.0
Integration			\$21.3	\$21.3
Subtotal			\$144.5	\$149.7

*Equipment quantities to be purchased with FY 2009 funds and carryover funds were reallocated for Whole Body Imagers, Advanced Technology and Credential Authentication Technology. However, the total quantity to be procured by the FY's end is unchanged.

	Initial FY 2009 Funds	Revised FY 2009 Funds
Program Operations and Management		
Logistics	\$12.3	\$7.3
Technical Engineering	\$4.1	\$4.1
Testing (IV&V)	\$3.3	\$3.3
Site Survey	\$3.2	\$3.2
Data Collection	\$3.0	\$3.0
TSA Systems Integration Facility	\$1.7	\$1.5
Program and Data Management	\$12.2	\$12.2
Travel, Training, Supplies	\$1.1	\$1.1
Subtotal, Program Operations and Management	\$40.9	\$35.7
Technical and Engineering Initiatives		
Security Technology Integration Program	\$8.0	\$7.6
Operational Integration of Emerging Technology	\$7.0	\$7.0
Threat Image Projection	\$4.0	\$4.0
Engineering Changes	\$2.0	\$2.4
Exit Lanes Data Collection	\$1.6	\$1.6
Subtotal, Technical and Engineering Initiatives	\$22.6	\$22.6

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

	Initial FY 2009 Funds	Revised FY 2009 Funds
Safety and Optimization		
Equipment	\$5.0	\$5.0
System Integrator	\$3.0	\$3.0
Engineering Support	\$2.5	\$2.5
Airport Projects	\$2.0	\$2.0
Project Logistics	\$1.0	\$1.0
Subtotal, Safety and Optimization	\$13.5	\$13.5
Checkpoint Reconfiguration		
Ancillary Equipment	\$3.0	\$3.0
Glass Partitions	\$2.7	\$2.7
Checkpoint Optimizations	\$1.7	\$1.7
Divest/Composure/Roller Tables	\$1.5	\$1.5
Project Logistics	\$1.5	\$1.5
Engineering and Technical Support	\$1.0	\$1.0
Travel	\$0.1	\$0.1
Subtotal, Checkpoint Reconfiguration	\$11.5	\$11.5
Advanced Surveillance Program		
Boston (BOS)	\$4.3	\$4.3
Orlando (MCO)	\$3.3	\$3.3
Philadelphia (PHL)	\$1.5	\$1.6
Phoenix (PHX)	\$1.0	\$0.0
Atlanta (ATL)	\$0.1	\$0.0
Chicago (ORD)	\$0.0	\$0.8
Cleveland (CLE)	\$0.0	\$0.1
Louis Munoz Marin (SJU)	\$0.0	\$0.1
Program Support	\$0.8	\$0.8
Subtotal, Advanced Surveillance Program	\$11.0	\$11.0
Personnel Compensation and Benefits		
Subtotal, Personnel Compensation and Benefits	\$6.0	\$6.0
Total	\$250.0	\$250.0

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix D: PSP Obligation Data

Spend Plan Categories	\$ in millions	Planned Obligation Date
Advanced Technology	\$63.5	Jul 2009
Universal Conveyor Systems	\$25.0	Aug 2009
Whole Body Imagers	\$12.2	Jul 2009
Credential Authentication Technology	\$9.0	Jul 2009
Bottled Liquids Scanners	\$7.5	Jul 2009
Explosives Trace Detectors	\$6.0	Jul 2009
Integration	\$21.3	Jul 2009
Program Operations and Management	\$40.9	Ongoing
Technical and Engineering Initiatives	\$22.6	Ongoing
Safety and Optimization	\$13.5	Ongoing
Checkpoint Reconfiguration	\$11.5	Ongoing
Advanced Surveillance Program	\$11.0	Ongoing
Personnel Compensation and Benefits	\$6.0	Ongoing
Subtotal	\$250.0	

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix E: PSP Milestones

Advanced Technology	
Initial Qualified Data Package Down Select	3/2009
QT&E Begins	3/2009
OT&E Begins	4/2009
Contract Award	7/2009
Universal Conveyor System	
QT&E Begins	TBD
OT&E Begins	TBD
Contract Award	8/2009
Whole Body Imagers	
QT&E Begins	2/2009
OT&E Begins	4/2009
Request For Proposals Released	6/2009
Contract Award	7/2009
Credential Authentication Technology	
Request For Proposals Released	3/2009
Contract Award	9/2009
Bottled Liquids Scanners	
OT&E Begins	3/2009
Contract Award	7/2009
Explosives Trace Detectors	
QT&E Began	11/2007
OT&E Began	3/2008
Contract Award	8/2008
Advanced Surveillance Program	
Boston (BOS)	5/2009
Orlando (MCO)	5/2009
Philadelphia (PHL)	5/2009
Chicago (ORD)	6/2009
Cleveland (CLE)	6/2009
Louis Munoz Marin (SJU)	6/2009

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix F: Actual vs. Anticipated Unobligated Balance
(as of 3/31/2009)

Spend Plan Category (\$ Million)	Budgeted	Obligated	Unobligated	Anticipated Unobligated end FY 2009
Checkpoint Technology	\$ 208.0	\$ 12.0	\$ 196.0	\$ 4.5
Checkpoint Reconfiguration	\$ 11.5	\$ 5.1	\$ 6.4	\$ -
ASP	\$ 11.0	\$ 0.0	\$ 11.0	\$ -
Safety Optimization	\$ 13.5	\$ 0.0	\$ 13.5	\$ -
PC&B	\$ 6.0	\$ 1.8	\$ 4.2	\$ -
Total	\$ 250.0	\$ 19.0	231.0	\$ 4.5

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY



Checkpoint Support and Explosives Detection Systems (EDS) Expenditure Plans

Fiscal Year 2009 Report to Congress

Third Quarter Update

November 12, 2009



Homeland
Security

Transportation Security Administration

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with

FOR OFFICIAL USE ONLY

Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Message from the Acting Administrator

November 12, 2009

I am pleased to present the "Checkpoint Support and Explosives Detection Systems (EDS) Expenditure Plans" update, which has been prepared by the Transportation Security Administration.

This quarterly report was required by the Fiscal Year 2009 Department of Homeland Security Appropriations Act (P.L. 110-329) and the accompanying Explanatory Statement and Senate Report 110-396. It provides an expenditure plan update for the procurement and installation of emerging technologies and advanced threat detection systems for airport passenger checkpoints and for the procurement and installation of EDS equipment. The report also includes updates on the use of funds provided by the American Recovery and Reinvestment Act (P.L. 111-5).

This report is being provided to the following Members of the Appropriations Committees:

The Honorable Robert C. Byrd
Chairman, Senate Appropriations Subcommittee on Homeland Security

The Honorable George V. Voinovich
Ranking Member, Senate Appropriations Subcommittee on Homeland Security

The Honorable David E. Price
Chairman, House Appropriations Subcommittee on Homeland Security

The Honorable Harold Rogers
Ranking Member, House Appropriations Subcommittee on Homeland Security

If I may be of further assistance, please do not hesitate to contact me at (571) 227-2845 or the Department's Acting Chief Financial Officer, Peggy Sherry, at (202) 447-5751.

Sincerely yours,



Gale D. Rossides
Acting Administrator

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Executive Summary

The Fiscal Year (FY) 2009 Department of Homeland Security Appropriations Act (P.L. 110-329) and the accompanying Explanatory Statement and Senate Report 110-396 requires the Transportation Security Administration (TSA) to submit quarterly updates on Explosive Detection Systems (EDS) and checkpoint expenditures. Checkpoint support funding is implemented through the Passenger Screening Program (PSP). TSA's checked baggage EDS purchase and installation funding is implemented through the Electronic Baggage Screening Program (EBSP).

Checkpoint Support

- PSP tests, procures, deploys, integrates, and provides life cycle support for security equipment to screen passengers and carry-on baggage at passenger checkpoint lanes at domestic airports. PSP is responsible for technologies that screen more than 700 million passengers per year at approximately 450 of the Nation's airports.
- The Advanced Surveillance Program (ASP) utilizes the existing infrastructure owned and operated by the transportation authority for remote monitoring, threat detection and assessment in a partnership agreement to provide enhanced situational awareness.
- Major updates in the third quarter include the following:
 - An additional \$11.1 million of American Recovery and Reinvestment Act (ARRA) funds added to checkpoint support for ASP/Closed Circuit Television (CCTV) projects
 - \$7 million included for Chemical Analyzer Detectors
 - \$18 million included for Credential Authentication Technology

Electronic Baggage Screening Program

- The EBSP oversees the screening of all baggage checked in airports nationwide. EBSP tests, procures, deploys, integrates and provides life cycle support for approximately 7,700 pieces of security equipment that screen checked baggage at approximately 450 of the Nation's airports.
- The EBSP allocates resources to airport baggage screening facility modification projects, purchase and installation of EDS technology and technology initiatives aimed at improving operational effectiveness and efficiencies, as well as the programmatic resources required to ensure effective execution of the program.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

- Major updates in the third quarter include the following:
 - FY 2009 funds were reallocated from Engineering Initiatives for the purchase of the TSA Systems Integration Facility building.
 - Through cost validation and negotiation, TSA was able to reduce projected costs for EDS airport projects from the original ARRA expenditure plan by almost \$310 million. Ten additional airports were added to the spend plan, and \$11.1 million was transferred from the EDS ARRA funds to finance checkpoint support for ASP/CCTV projects.
 - \$38.4 million of the EDS funds will be used for ASP/CCTV projects in the checked baggage area of the airport.
 - An additional \$30 million of the EDS funds will be used to procure and install Reduced Size EDSs to Explosives Trace Detection (ETD)-only airports to improve operational efficiencies and screening effectiveness.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.



Checkpoint Support and Explosives Detection Systems (EDS) Expenditure Plans 3rd Quarter Update, Fiscal Year 2009

Table of Contents

I. Legislative Requirement	1
II. Passenger Screening Program (PSP)	2
A. Background	2
B. Expenditure Plan	4
C. Program Initiatives	6
III. Electronic Baggage Screening Program (EBSP)	13
A. Background	13
B. Expenditure Plan	16
IV. Appendices	23
Appendix A. Abbreviations/Acronyms	23
Appendix B. Airport Codes	25
Appendix C. Passenger Screening Program (PSP) Deployments by Airport	31
Appendix D. PSP FY 2009 Summary Spend Plan	35
Appendix E. PSP American Recovery and Reinvestment Act (ARRA) Summary Spend Plan	38
Appendix F. PSP FY 2009 Obligation Data	40
Appendix G. PSP ARRA Obligation Data	41
Appendix H. PSP FY 2009 Milestones	42

FOR OFFICIAL USE ONLY

Appendix I.	PSP ARRA Milestones	43
Appendix J.	PSP FY 2009 Actual vs. Anticipated Unobligated Balance, as of June 30, 2009	45
Appendix K.	PSP ARRA Actual vs. Anticipated Unobligated Balance, as of June 30, 2009	46
Appendix L.	Electronic Baggage Screening Program (EBSP) FY 2009 Obligation by Project	47
Appendix M.	EBSP ARRA Obligation by Project	50
Appendix N.	EBSP FY 2009 Summary Spend Plan	51
Appendix O.	EBSP ARRA Summary Spend Plan	59
Appendix P.	EBSP FY 2009 Obligation Data	68
Appendix Q.	EBSP ARRA Obligation Data	76
Appendix R.	EBSP FY 2009 Milestones	77
Appendix S.	EBSP ARRA Milestones	88

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

I. Legislative Requirement

The Fiscal Year (FY) 2009 Department of Homeland Security (DHS) Appropriations Act (P.L. 110-329) and the accompanying Explanatory Statement and Senate Report 110-396, includes the following requirement:

Aviation Security—Explosive Detection Systems

TSA shall provide an expenditure plan to the Committees not later than 60 days after the date of enactment of this Act, as discussed under Transportation Security Support. If new requirements occur after the plan is submitted, TSA shall reassess and reallocate funds after notifying the Committees of any change. As discussed in the Senate report, TSA shall provide quarterly updates on EDS and checkpoint expenditures, on an airport-by-airport basis. These updates shall include information on the specific technologies for purchase, project timelines, a schedule for obligation, and a table detailing actual versus anticipated unobligated balances at the close of the fiscal year, with an explanation of any deviation from the original plan.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

II. Passenger Screening Program (PSP)

A. Background

Mission

PSP's Mission Need supports prevention and protection from terrorist and criminal actions in the aviation transportation environment. PSP specifically focuses on technology and processes utilized in and near the passenger screening checkpoint to achieve the air travel passenger security mission. PSP's mission includes being responsible for the acquisition of technology that identifies threats concealed on people and their carry-on items entering the sterile area of the airport terminal through the passenger screening checkpoint. The checkpoint is defined as the screening equipment, processes and operating personnel collectively required to perform the security mission.

Purpose

PSP accomplishes its mission by identifying, testing, procuring, deploying, integrating and sustaining equipment that identifies threats concealed on passengers and their carry-on items as they enter the airport terminal through the passenger screening checkpoint.

Goals

PSP supports Goal One of the DHS Strategic Plan, FY 2008-2013, "Protect Our Nation from Dangerous People."

PSP Objectives:

- **Explosives Detection:** Detect explosives threats, weapons and other prohibited items concealed on passengers and their carry-on items.
- **Screening Efficiency:** Improve checkpoint efficiency through process automation.
- **Layered Security:** Enable a layered, integrated security solution.

The following are accomplishments of PSP technologies:

- **Advanced Technology (AT) X-Ray.** More than 850 AT (first-generation) operational units deployed nationwide have expanded the capabilities of the Transportation Security Officers (TSOs) at the checkpoint; these units replace legacy Threat Image Projection (TIP) Ready X-Ray (TRX) systems. AT systems are penetration x ray-based technologies that provide an enhanced view of a bag's contents through improved image resolution. Also, an added dimension to the displayed image provides better material discrimination for TSOs to discern each object inside a bag. AT systems are

FOR OFFICIAL USE ONLY

upgradeable, offering a cost-effective platform to develop enhanced detection capabilities. Additionally, AT systems can include the universal conveyor system (UCS), which diverts bags requiring a secondary search. The UCS will assist in maintaining positive control of and tracking all passenger carry-on baggage until the screening technology clearly indicates the baggage's status and a TSO decides to deliver the baggage to the passenger. This functionality will improve overall throughput and minimize congestion on the exit side of the AT system. Deployments are ongoing and the second generation of AT will undergo testing in the fourth quarter of FY 2009.

- **Advanced Imaging Technology (AIT).** Previously known as whole body imaging or WBI, AIT is a new imaging capability that will be used to inspect a passenger for concealed weapons (metal and non-metal), explosives and other prohibited items. In addition, the AIT offers operators the opportunity to review anomalies on an individual to determine if a physical pat-down inspection is required. AITs could ultimately be the primary passenger screening technology instead of using an Enhanced Metal Detector (EMD). The Transportation Security Administration (TSA) has assessed two types of technologies for the AITs, including x ray backscatter and millimeter wave technology. Both offer safe and effective screening for weapons and explosives concealed on a person. Deployments are ongoing and the second generation of AIT will undergo testing in the fourth quarter of FY 2009.
- **Bottled Liquid Scanner (BLS).** A BLS offers detection capability that can discriminate explosives or flammable liquids from common, benign liquids carried by passengers. The device analyzes substances within a container (bottle or can), measuring particular characteristics of the contents and distinguishing between benign and hazardous liquids in seconds. The second-generation devices perform scans without breaking seals or contaminating passengers' property and will greatly reduce annual consumable costs.
- **Credential Authentication Technology/Boarding Pass Scanning Systems (CAT/BPSS).** CAT/BPSS provides a common platform for automated credential authentication and boarding pass validation. First-generation systems will allow the TSA to verify that forms of identification presented to gain access to sterile areas in airports are genuine documents and that boarding passes have been issued by a valid airline and no tampering with the data stored on the boarding pass has occurred. Second-generation systems will allow the TSA to compare data from passengers' identification to data stored in the 2D barcode on the boarding pass. Second-generation systems will also feature an expanded library of airport, airline and law enforcement identification. CAT/BPSS units will provide the TSA with increased control of access to airport sterile areas. CAT/BPSS recently completed pilot programs at Ronald Reagan Washington National Airport and Baltimore/Washington International Thurgood Marshall Airport as part of the current solicitation.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

- **Chemical Analyzer Detector (CAD).** CADs will be used to assess suspicious substances in the possession of people passing through security checkpoints. Bomb Appraisal Officers (BAOs) will respond to requests by screener personnel for advanced alarm resolution (that is, secondary offline screening) of liquids, powders and solid suspicious substances at the airport and other designated security checkpoints.

The following chart shows enacted amounts since inception of the Checkpoint Support Program, Project and Activity (PPA). Values are in millions of dollars.

2002	2003	2004	2005	2006	2007	07 supp	2008	2009	ARRA	TOTAL
\$ 38.00	\$ 40.00	\$ 61.86	\$123.50	\$164.00	\$173.37	\$ 25.00	\$250.00	\$245.20	\$311.15	\$1,432.08

B. Expenditure Plan

Summary of PSP Expenditure Plan (dollar amounts in millions)

Section	FY09 Approved	ARRA Approved	Total Approved	FY09 Revised	ARRA Revised	Total Revised
Technology	\$ 149.70	\$ 197.70	\$ 347.40	\$ 113.10	\$ 202.90	\$ 316.00
Program Operations and Management	\$ 35.70	\$ 82.90	\$ 118.60	\$ 63.50	\$ 77.70	\$ 141.20
Technical and Engineering Initiatives	\$ 22.60	\$ 9.90	\$ 32.50	\$ 26.60	\$ 9.90	\$ 36.50
Safety and Optimization	\$ 13.50	\$ -	\$ 13.50	\$ 13.50	\$ -	\$ 13.50
Checkpoint Reconfiguration	\$ 11.50	\$ -	\$ 11.50	\$ 11.50	\$ -	\$ 11.50
Advanced Surveillance Program	\$ 11.00	\$ 5.70	\$ 16.70	\$ 11.00	\$ 16.85	\$ 27.85
Personnel Compensation and Benefits	\$ 6.00	\$ 3.80	\$ 9.80	\$ 6.00	\$ 3.80	\$ 9.80
Total	\$ 250.00	\$ 300.00	\$ 550.00	\$ 245.20	\$ 311.15	\$ 556.35

FY09 Revised: Total lower due to funds being reallocated to another PPA.

ARRA Revised: Total higher, additional airports to be served by ASP

FY 2009 reallocations were necessary to account for additional integration requirements of the emerging technologies. American Recovery and Reinvestment Act of 2009 (ARRA) changes include the addition of the CADs, CAT and airports for the Advanced Surveillance Program (ASP). UCS was lowered by approximately 50 units to account for added integration requirements and to procure additional explosives trace detectors.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Technology Purchases and Percentages to Reach Full Operational Capability (FOC)

Technology	FOC	Purchases with Prior Year Funds	Prior Years	Purchases with FY09 Funds	FY09	Purchases with ARRA Funds	ARRA	PURCHASES TOTAL	TOTAL % of FOC
Advanced Technology ¹	2325	1029	44%	488	65%	611	92%	2128	92%
Universal Conveyor Systems	2325	0	0%	0	0%	228	10%	228	10%
Advanced Imaging Technology	878	47	5%	175	25%	200	48%	422	48%
Credential Authentication Technology	2325	0	0%	0	0%	800	34%	800	34%
Bottled Liquids Scanners	1300	200	15%	600	62%	500	100%	1300	100%
Explosives Trace Detectors	1500	100	7%	0	7%	400	33%	500	33%
Chemical Analyzer Detector	140	0	0%	0	0%	140	100%	140	100%

¹ Percentage of FOC based on FY14 estimates.

Checkpoint Support Expenditure Plan

PROGRAM SPENDING PLAN: Checkpoint Support

APPROPRIATIONS IN \$ MILLIONS

Net Appropriated Funds	556.350
Funds Obligated	35.507
Project Outlays	7.141
Unobligated Balance	520.843

UNOBLIGATED BALANCES BY FY

FY09/ARRA	Total
520.843	520.843

OBLIGATIONS IN \$ MILLIONS

	Q1FY09	Q2FY09	Q3FY09	Q4FY09	FY10	FY11	FY12	FY13	FY14
Plan	16.260	40.280	218.510	276.410	4.890	-	-	-	-
Plan Cumulative	16.260	56.540	275.050	551.460	556.350	-	-	-	-
Cumulative % Allotment	0.00%	21.91%	12.21%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Actual	-	8.825	26.682	-	-	-	-	-	-

OUTLAYS IN \$ MILLIONS

	Q1FY09	Q2FY09	Q3FY09	Q4FY09	FY10	FY11	FY12	FY13	FY14
Plan	-	8.000	22.650	54.270	480.430	-	-	-	-
Plan Cumulative	-	8.000	30.650	84.920	565.350	-	-	-	-
Cumulative % Allotment	0.00%	24.79%	22.77%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
Actual	-	1.983	5.158	-	-	-	-	-	-

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

C. Program Initiatives

Description of Initiative I – AT X-Ray

- AT systems are penetration x ray-based technologies that provide an enhanced view of a bag's contents through improved image resolution beyond the capabilities of the currently fielded TRX equipment. Also, an added dimension to the displayed image provides better material discrimination for TSOs to discern each object inside a bag. AT offers a cost-effective platform to develop enhanced detection capabilities. Future enhancements may include an enhanced conveyor system. More than 850 first-generation AT units are being deployed and installed at airports nationwide. The second generation of AT with upgraded capability and functionality is in the development stage.
- Obligations to date: \$106.6 million
- Projected FY 2009 obligations by year: FY 2009 – \$0, FY 2010 – \$61.0 million
- Projected FY 2009 expenditures: FY 2010 – \$61.0 million
- Projected ARRA obligations by year: FY 2009 – \$2.9M, FY 2010 – \$73.5 million
- Projected ARRA expenditures by year: FY 2009 – \$2.9 million, FY 2010 – \$73.5 million
- Major performance objectives:
 - Probability of detection of threat items: Classified
 - Throughput: ≥ 440 bags per hour with operator intervention
 - Operational availability: ≥ 98 percent
- Activities and milestones/accomplishments:
 - Initial Operational Capability (IOC): Q3 FY 2008
 - Qualification Testing and Evaluation (QT&E): Q4 FY 2009
 - Operational Testing and Evaluation (OT&E): Q4 FY 2009
 - Contract award: Q1 FY 2010
 - FOC: Q1 FY 2011 accelerated from Q2 FY 2014

Description of Initiative II – UCS

- UCSs are carry-on baggage handling conveyor systems added to the AT systems to support automated diversion of alarm bags from cleared baggage.
- Obligations to date: \$0
- Projected ARRA obligations: FY 2010 – \$28.5 million
- Projected ARRA expenditures by year: FY 2010 – \$8.5M, FY 2011 – \$20.0 million
- Activities and milestones/accomplishments:
 - Contract award: Q2 FY 2010
 - IOC: Q2 FY 2010

FOR OFFICIAL USE ONLY

Description of Initiative III – AIT

- AIT provides an imaging capability used to inspect a passenger's body for concealed weapons (metal and nonmetal), explosives and other prohibited items in place of a metal detection wand inspection and physical pat-down. The AIT could potentially become a primary screening technology, which could be used in conjunction with, or instead of, an EMD.
- Obligations to date: \$13.6 million
- Projected FY 2009 obligations: FY 2009 – \$28.9 million
- Projected FY 2009 expenditures: FY 2010 – \$28.9 million
- Projected ARRA obligations: FY 2009 – \$32.2 million
- Projected ARRA expenditures: FY 2010 – \$32.2 million
- Major performance objectives:
 - Probability of threat detection: Classified
 - Throughput: ≥ 200 passengers per hour
 - Operational availability: ≥ 98 percent
- Activities and milestones/accomplishments:
 - QT&E: Q4 FY 2009
 - OT&E: Q4 FY 2009
 - Contract award: Q4 FY 2009
 - IOC: Q4 FY 2009
 - FOC: Q4 FY 2014

Description of Initiative IV – CAT

- The CAT system provides a primary means for automated verification of passenger travel documents and forms of identification that passengers present to TSOs during the security checkpoint screening process, as well as those forms of identification presented by airport and airline personnel to access sterile areas. This system will increase TSOs' abilities to locate fraudulent IDs and validate the issuing authority and authenticity of boarding passes at security checkpoints.
- Obligations to date: \$0
- Projected ARRA obligations: FY 2009 – \$18.0 million
- Projected ARRA expenditures: FY 2010 – \$18.0 million
- Activities and milestones/accomplishments:
 - Request for proposals: Q3 FY 2009
 - Contract award: Q4 FY 2009
 - FOC: Q2 FY 2011

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Description of Initiative V – **BLS**

- A BLS is an Explosives Detection System (EDS) that differentiate liquid explosives from common, benign liquids. BLS utilize a variety of technologies to detect liquid explosives and explosive precursors, including vapor detection, x ray detection, detection using the dielectric properties of the materials being scanned or optical detection using Raman spectroscopy.
- Obligations to date: \$0
- Projected FY 2009 obligations: FY 2009 – \$22.7 million
- Projected FY 2009 expenditures: FY 2010 – \$22.7 million
- Projected ARRA obligations: FY 2009 – \$18.8 million
- Projected ARRA expenditures: FY 2010 – \$18.8M
- Major performance objectives:
 - Probability of detection of threat items: Classified
 - Throughput: ≥ 180 samples per hour
 - Operational availability: ≥ 98 percent
- Activities and milestones/accomplishments:
 - IOC To Be Determined (TBD): Q1 FY 2010
 - QT&E: Q3 FY 2009
 - OT&E: Q4 FY 2009
 - Contract award: Q4 FY 2009
 - FOC: Q1 FY 2011

Description of Initiative VI – **Next Generation (Next Gen) ETD**

- Next Gen ETDs identify a larger range of explosives than earlier models. The Next Gen ETDs have enhanced explosives detection capability, including increased sensitivity and the ability to detect new threats. The Mean Time to Repair will be significantly less than for the current ETD technology. In addition, the Next Gen ETDs will have a Field Data Reporting System and will be Security Technology Integration Program capable. Because of these significant improvements, a lower life cycle cost is expected.
- Obligations to date: \$6.1 million
- Projected FY 2009 obligations: FY 2009 – \$0.5 million
- Projected FY 2009 expenditures: FY09 – \$0.5 million
- Projected ARRA obligations: FY 2009 – \$22.0 million
- Projected ARRA expenditures: FY 2010 – \$22.0 million
- Major performance objectives:
 - Probability of detection of threat items: Classified
 - Throughput: 180 samples per hour, to include machine processing and analysis, when no alarms are present
 - Operational availability: ≥ 98 percent
- Activities and Milestones/Accomplishments:
 - QT&E: Q1 FY 2008

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

- OT&E: Q2 FY 2008
- Contract award: Q4 FY 2008
- IOC: Q1 FY 2009
- FOC: Q4 FY 2014

Description of Initiative VII – CADs

- CADs are portable systems that can be used by BAOs and Explosives Security Specialists (ESS) to identify a range of chemical agents, precursors and explosives threats quickly. These devices will be used to assess suspicious substances in the possession of passengers traveling through the security checkpoints.
- Obligations to date: \$0.25 million
- Projected FY 2009 obligations: FY 2009 – \$0
- Projected FY 2009 expenditures: FY 2009 – \$0
- Projected ARRA obligations by year: FY 2009 – \$0.25 million; FY 2010 – \$6.75 million
- Projected ARRA expenditures: FY 2010 – \$7.0 million
- Major performance objectives:
 - Probability of detection of threat items: Classified
 - Operational availability: ≥ 96 percent
- Activities and Milestones/Accomplishments:
 - QT&E: Q4 FY 2009
 - OT&E: Q1 FY 2010
 - Contract award: Q1 FY 2010
 - IOC: Q1 FY 2010
 - FOC: Q4 FY 2010

Description of Initiative VIII – Integration

Relates to all tasks associated with the installation of security technology equipment at geographically dispersed airports nationwide.

- **Integration** services can include moving equipment, small-scale facility modification or electrical and plumbing repairs.
- **Project Logistics** deal with the procurement, distribution and replacement of systems to and from the field.
- **Installation and Design** services encompass architectural design and review, site survey and construction package review.
- Projected FY 2009 obligations: FY 2009 – \$31.9 million
- Projected FY 2009 expenditures by year: FY 2009 – \$15.0 million; FY 2010 – \$16.9 million
- Projected ARRA obligations: FY 2009 – \$68.2 million
- Projected ARRA expenditures: FY 2010 – \$68.2 million

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Description of Initiative IX – **Program Operations and Management**

Program Operations and Management encompasses activities needed for the procurement and deployment of security systems to the Nation's airports. The following activities make up this initiative:

- **Engineering Support** encompasses requirements review, technical representation and technical management support.
- **Independent Verification and Validation** encompasses factory acceptance testing, site acceptance testing and integrated site testing.
- **Data Collection** activities are those associated with documentation, reports and technical support of testing.
- **TSA Systems Integration Facility** provides an operationally realistic environment to evaluate current/new advanced screening technologies, processes and procedures against known threats to transportation venues, particularly air transportation venues.
- **Program Resource and Data Management** activities encompass project management support, financial management and analysis, data management and project scheduling.
- Projected FY 2009 obligations: FY 2009 – \$31.6 million
- Projected FY 2009 expenditures by year: FY 2009 – \$20.0 million; FY 2010 – \$11.6 million
- Projected ARRA obligations by year: FY 2009 – \$2.0 million, FY 2010 – \$7.5 million
- Projected ARRA expenditures: FY 2010 – \$9.5 million

Description of Initiative X – **Technical and Engineering Initiatives**

- **Security Technology Integration Program** is an agencywide system that enables TSA to connect all Transportation Security Equipment to one data management system that will facilitate the exchange of information across the network and facilitate maintenance servicing and diagnostic information.
- **Operational Integration (OI) of Emerging Technology** consists of data collection, research and field tests to verify systems, operational innovations and screening upgrades in a variety of conditions, climates and processes. Reliability, maintainability and availability will be assessed on new technologies and innovations so that decisions concerning their deployability and usefulness can be effectively made. Examples of emerging technologies to be field tested and piloted include AIT, AT, BLS and CAT (including passenger wait-time collection pilot).
- **TIP** keeps TSOs alert and exposes them to a variety of prohibited item images they may not normally see. It is also used as an evaluation tool to assess a TSO's visual inspection performance of detecting prohibited items during real working hours instead of in lab conditions.
- **Engineering Changes** are required to modify technology to support enhanced capabilities such as throughput, detection, operator interface, and so on.
- **Exit Lane Breach Control** tests and evaluates the performance capabilities and technical viability of technologies that minimize the risk of unauthorized access and reduce resource requirements at exit lanes.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

- Projected FY 2009 obligations: FY 2009 – \$26.6 million
- Projected FY 2009 expenditures by year: FY 2009 – \$15.0 million; FY 2010 – \$11.6 million
- Projected ARRA obligations: FY 2010 – \$9.9 million
- Projected ARRA expenditures: FY 2010 – \$9.9 million

Description of Initiative XI – Safety and Optimization

- The Safety and Optimization Program improves the safety and efficiency of checkpoints and checked baggage screening operations by deploying ancillary equipment and enhancing the design and layout of screening areas.
- Funding will be used to procure equipment and services to complete airport safety enhancement projects to minimize the amount of TSOs injured on the job.
- Projected FY 2009 obligations: FY 2009 – \$13.5 million
- Projected FY 2009 expenditures by year: FY 2009 – \$9.0 million; FY 2010 – \$4.5 million

Description of Initiative XII – Checkpoint Reconfiguration

- Checkpoint reconfigurations are required at airports to maintain or improve throughput due to the growth in passenger traffic and the evolution of the airline industry. Reconfiguration of checkpoints can also be required as emerging technologies are deployed to efficiently utilize the checkpoint space.
- Funding will be used to procure glass for wand stations, adjustable divest and composure tables and ancillary equipment for checkpoints such as podiums and benches, as well as to reconfigure checkpoint equipment and layouts to accommodate emerging technologies and redesign to make checkpoints more efficient.
- Projected FY 2009 obligations: FY 2009 – \$11.5 million
- Projected FY 2009 expenditures by year: FY 2009 – \$4.0 million, FY 2010 – \$7.5 million

Description of Initiative XIII – ASP

- ASP utilizes the existing infrastructure owned and operated by the transportation authority for remote monitoring, threat detection and assessment in a partnership agreement to provide enhanced situational awareness of the checkpoint and checked baggage area of airports.
- Obligations to date: about \$48.0 million
- Projected FY 2009 obligations: FY 2009 – \$11.0 million
- Projected FY 2009 expenditures: FY 2010 – \$11.0 million
- Projected ARRA obligations: FY 2009 – \$16.8 million
- Projected ARRA expenditures: FY 2010 – \$16.8 million

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

- Activities and Milestones/Accomplishments:
 - Site visits: TBD by airport
 - Proposals: Q3 FY 2009
 - Contract awards: Q4 FY 2009

Description of Initiative XIV – Personnel Compensation and Benefits (PC&B)

- Projected FY 2009 expenditures: FY 2009 – \$6.0 million
- Projected ARRA expenditures: FY 2010 – \$3.8 million

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

III. Electronic Baggage Screening Program (EBSP)

A. Background

Mission

EBSP's mission is central to the TSA security mission area because it covers: *"The range of TSA activities that minimize the risk of injury or death of people or damage or loss of property due to hostile acts of terrorism that may be directed against the National Airspace System."*

Preventing catastrophic loss and air piracy involves verifying that checked baggage carries no prohibited items or items that have been identified as threat objects for the particular transportation mode. The screening process targets the checked baggage of all people boarding aircraft through the use of screening security systems.

EBSP tests, acquires, deploys, integrates and maintains the technology that screens passenger-checked baggage to deter, detect, mitigate and prevent transportation of explosives or other prohibited items on commercial aircraft while ensuring freedom of movement for people and commerce.

Purpose

EBSP was initiated by the White House Commission on Aviation Safety and Security at the Federal Aviation Administration in 1997. In response to the events of September 11, 2001, a Congressional mandate transferred the EBSP to DHS. Furthermore, public laws were enacted to accelerate and dramatically increase the scope of the EBSP. The Aviation and Transportation Security Act (ATSA), P.L. 107-71, stated that all checked baggage must be screened at all the nation's airports with an EDS or a suitable alternative as soon as possible but not later than December 31, 2002. The Homeland Security Act of 2002 (HSA), P.L. 107-296, later granted DHS a waiver until December 31, 2003, to screen all checked baggage at all airports, a condition that was met.

EBSP is currently in a "mixed" acquisition life cycle, focusing predominately on the purchase, deployment and sustainment phases of the acquisition process. The primary technologies acquired and deployed under the EBSP are EDS equipment and ETD devices. The following three technology configurations comply with the mandates of ATSA and the HSA:

1. ETD-based Systems – TSOs use ETD machines as a primary method to screen bags.
2. Standalone EDSs – TSOs use EDS machines as a primary method to screen bags. Alarmed bags are resolved by ETDs.

FOR OFFICIAL USE ONLY

3. Inline EDS Systems – TSOs use EDS machines as a primary method to screen bags. Alarmed bags are resolved by ETDs.

Using EDS technology (both inline and standalone) is preferred over using ETDs as a primary screening method because of the following:

1. (b)(3);49 U.S.C. § 114(r) detailed performance capabilities are classified). Improving security supports TSA and DHS goals to prevent and protect.
2. Increased Efficiency – EDS machines have a higher throughput than ETD units used in primary screening, which decreases lobby congestion and passenger wait time. Higher baggage throughput supports TSA's goal of "ensuring freedom of movement for people and commerce."
3. Decreased Labor Costs – EDS configurations at larger airports require fewer TSOs to operate than ETDs used in primary screening configurations. Increased automation reduces human error and personnel costs. EDS machines also have reduced operating costs over the life of the equipment and require less lifting of baggage, thus reducing the number of on-the-job injuries.

These technologies have been in production since 1997, and production is expected to continue indefinitely with enhancements both to engineering and detection capabilities. EBSP currently manages seven technology vendors and 16 technology models and provides life-cycle procurement, deployment, integration and maintenance of more than 7,700 units of security equipment at approximately 450 U.S. Federalized airports. To date, EBSP has supplied 68 airports with full optimal systems and enabled some screening areas with optimal systems at 52 additional airports.

The following chart shows the enacted/appropriated funding since inception of the EDS/ETD Install and Purchase PPA. Values are in millions of dollars.

Program Project and Activity	2002	02 Supp	2003	03 Supp	2004	2005	2006	2007	07 Supp	2008	2009	ARRA	TOTAL
EDS/ETD Purchase	\$859.80	\$0.00	\$174.50	\$0.00	\$150.00	\$180.00	\$175.00	\$141.40	\$55.44	\$103.63	\$107.70	\$60.00	\$2,007.47
EDS/ETD Installation	\$0.00	\$738.00	\$265.00	\$235.00	\$250.00	\$295.00	\$295.00	\$388.00	\$229.56	\$440.37	\$436.30	\$628.85	\$4,201.23
Total	\$859.80	\$738.00	\$439.50	\$235.00	\$400.00	\$475.00	\$470.00	\$529.40	\$285.00	\$544.00	\$544.00	\$688.85	\$6,208.70

* Includes the Aviation Security Capital Fund (ASCF) Fee beginning FY 2007

Goal

The EBSP supports Goal Two of the DHS Strategic Plan, FY 2008-2013, "Protect Our Nation from Dangerous Goods."

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

EBSP fulfills the congressional mandate for 100 percent screening of aviation checked baggage by electronic or other approved means (found in ATSA Section 110).

The mandate to screen 100 percent of checked baggage has been achieved, and ongoing efforts to operate, maintain and improve screening systems remains critical. In particular, it is imperative that the program continue to research, evaluate and deploy refinements to EDS and ETD technology and associated systems that allow for improvements in (1) throughput (checked bags per hour), (2) the false alarm rate, (3) system availability and (4) total cost of ownership for baggage screening (cost per checked bag). In addition, it is desirable to relocate equipment from airport lobby areas to baggage room areas.

Program progress to date relative to EDS/ETD deployment and facility modifications

EDS/ETD Purchases
Historical Funding (FY 2004 through FY 2009)
Dollars in Thousands

	Purchase	Install	Units/EDSs	Units/ETDs	Agreements	% Agreements Awarded*	% Install Awarded**
FY 2004							
Enacted	149,700	249,000	136	24	19	100	100
FY 2005							
Enacted	180,000	295,000	134	248	3	100	100
FY 2006							
Enacted	175,000	295,000	216	552	17	100	100
FY 2007							
Enacted***	141,400	388,000	133	529	7	100	100
FY 2007							
Supplemental							
Enacted***	55,440	229,560	48	0	6	100	100
FY 2008							
Enacted***	103,627	440,373	114	3	10	100	95
FY 2009							
Enacted***	107,700	436,300	129	0	11	0	86
ARRA	60,000	628,850	160	0	26	11	28

*Agreements awarded: percent of planned project Other Transactional Agreements (OTAs)/Letters of Intent (LOIs) awarded either in the year funding was appropriated or the following year with carryover funding

**Installs awarded: percent of planned airport projects completed with EDS/ETD purchased and installed equipment either in the year funding was appropriated or the following year with the available carryover funding. The FY 2008 planned purchase and installation projects will be completed in FY 2009 with available carryover funding.

***Includes \$250 million Aviation Security Capital Fund fees

Per congressional direction, EBSP allocates funding among a wide variety of airports ranging from non-hub to large. Funding provided to EBSP by the ARRA will reduce the timeline for reaching the optimal solution at all airports by up to 2-3 years. When EBSP nears the achievement of its optimal solution, funding allocation will begin to shift from primarily

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

purchase and install costs to operations and management and recapitalization costs as the need for new installations decreases.

The TSA is currently planning to enter into letters of intent (LOI) negotiations with airports in Los Angeles, CA; Washington, DC; Tallahassee, FL and Fort Lauderdale, FL, for FY 2010. This early communication with the selected airports will ensure that TSA continues with the expedited deployment of EDSs to maintain a high level of system efficiency and effectiveness by decreasing threats.

B. Expenditure Plan

Summary of EBSP Expenditure Plan

Section	FY09 Approved	ARRA Approved	Total Approved	FY09 Revised	ARRA Revised	Total Revised
Program Operations and Management	\$74.9	\$32.0	\$106.9	\$97.5	\$54.85	\$152.35
LOI	\$200.0	\$0.0	\$200.0	\$200.0	\$0.0	\$200.0
OTA/New Facility Modification Agreement Projects	\$82.5	\$598.1	\$680.6	\$67.3	\$499.2	\$566.5
EDS Purchase and Install	\$146.6	\$64.2	\$210.8	\$146.6	\$94.2	\$240.8
Technology/Engineering Initiatives	\$40.0	\$5.7	\$45.7	\$32.6	\$40.6	\$73.2
Total	\$544.0	\$700.0	\$1244	\$544.0	\$688.85	\$1232.85

FY 2009

The FY 2009 Spend Plan totals \$544 million in FY 2009 enacted level:

- Total FY 2009 Purchase Funds equal \$107.7 million of enacted FY 2009 funds
- Total FY0 209 Install Funds equal \$436.3 million, which includes \$186.3 million of enacted FY 2009 funds and \$250 million Airport Security Capital Funds

Total project costs represent incurred costs: original equipment procurement, manufacturer installation, integration, multiplexing, warehousing, shipping, testing and facility modifications.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Facility modification amounts are based on FY 2009 application information and TSA cost validation process. The amount is subject to change because of updated cost submittals and negotiations with the airport.

TSA has identified a total of three LOIs, eight airports for facility modifications and 42 airports for Purchase and Installations.

ARRA

Based on the established long-term EDS Strategic Planning Framework, plus airport-specific project information, EBSP submits a revised ARRA spend plan totaling \$688.85 million for the purchase of EDS equipment, installation of EDS equipment and facility modifications to airports to accommodate the EDS equipment. The original plan was submitted with \$700 million for this program, but further organizational review revealed a need to support ASP and resulted in a reallocation of \$11.15 million to PSP, resulting in a reduction of the EDS allocation.

Total project costs represent the following incurred costs: original equipment procurement, manufacturer installation, integration, multiplexing, warehousing, shipping, testing and facility modifications.

Facility modifications are based on initial applications and the TSA cost validation process. The amount is subject to change because of updated cost submissions and negotiations with the airports.

The 16 airports identified to receive the first infusion of ARRA funds from TSA were selected from a pool of completed applications originally submitted for FY 2009 funding, but which remained unfunded because of resource limitations. The 16 airports had already provided complete applications, enjoyed proactive airport administrations and represented a cross-section of mid- to larger-size airports. Also, when taken together, the 16 airports comprised a significant percentage of passenger traffic, hence yielding excellent security enhancement value for the amount of ARRA funds identified. Of the original 16 airports which agreed to participate, one airport (Tallahassee) has since withdrawn.

The original ARRA spend plan reflected a total cost of about \$598 million for facility modifications, while revised projected costs totaled approximately \$499.2 million. Ultimately, through the process of cost validation and negotiation, TSA was able to reduce the total projected costs for EDS airport projects from the original ARRA spend plan by more than \$80 million while also adding 10 airport projects. The savings achieved will allow the EBSP to improve the security and efficiency of the screening process at these 10 airports, which had cost-validated plans in place but were previously deferred to FY 2010 and beyond.

TSA identified 10 airports as potential candidates for these additional EDS airport projects. All would be able to accept the funding in the accelerated cycle and complete their proposed projects

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

in the allowable time frames. The total cost for the 10 additional airports is \$243 million. The 10 additional airports are:

- Lambert-Saint Louis International, St. Louis, MO
- Washington Dulles International, Chantilly, VA
- Yellowstone Regional, Cody, WY
- William P. Hobby, Houston, TX
- St. Petersburg-Clearwater International, St. Petersburg, FL
- Gallatin Field, Bozeman, MT
- Little Rock National, Little Rock, AR
- Tulsa International, Tulsa, OK
- Charlotte/Douglas International, Charlotte, NC
- Colorado Springs, Colorado Springs, CO

Program support will increase to accommodate the added projects. The TSA will increase Full Time Position staffing via the current hiring flexibilities available to agencies. Additional contract support personnel are also required to assist with site surveys/visits, airport outreach support, equipment testing and evaluation, and program management support.

TSA also will increase the procurement and deployment of Reduced Size EDSs by \$30 million to ETD-only airports to improve screening effectiveness and operational efficiencies.

Supporting Data

Estimated Number of Airports with Optimal Systems

Category	Total Number of TSA Airports	Entire Airport with Optimal Systems	Some Screening Areas with Optimal Systems	Total Number of Airports with at least one Optimal System	% of Airports with at least one Optimal System	Optimal Systems Inline Projects Funded FY 2009*	Optimal Systems Inline Projects Funded ARRA*
X	27	5	17	22	81%	2	9
I	55	15	17	32	58%	3	10
II	73	27	15	42	58%	6	5
III	122	21	3	24	20%	21	20
Total	277	68	52	120	43%	41	44

*FY 2009 and ARRA funds include Reduced Size EDS purchase for ETD-only airports.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

EBSP Expenditure Plan

Expenditure Plan: Appropriations, Obligations, and Expenditures

PROGRAM SPENDING PLAN: EBSP

APPROPRIATIONS IN \$ MILLIONS

Net Appropriated Funds ¹	1,232.85
Project Outlays End-of-Q1 FY09	109.01
Funds Obligated, Not Outlaid End-of-Q1 FY FY09	63.99
Unobligated Balance End-of-Q1 FY09	1,077.60

UNOBLIGATED BALANCES BY FY as of 30 JUNE 2009

FY09	Total
1,077.595	1,169.359

PLANNED OBLIGATIONS IN \$ MILLIONS AS OF 30 JUNE 2009

	Q1FY09	Q2FY09	Q3FY09	Q4FY09	Q1FY10	Q2FY10	Q3FY10	Q4FY10
Plan	18.727	70.074	359.865	638.577	145.768	-	-	-
Plan Cumulative	18.727	88.801	448.667	1,087.244	1,233.012	n/a	n/a	n/a
Cumulative % Allotment	10.30%	55.92%	24.08%	0.00%	0.00%			
Actual	1.929	39.183	86.655	-	-	-	-	-

PLANNED OUTLAYS IN \$ MILLIONS AS OF 30 JUNE 2009

	Q1FY09	Q2FY09	Q3FY09	Q4FY09	Q1FY10	Q2FY10	Q3FY10	Q4FY10
Plan	18.727	52.556	250.925	216.311	680.666	13.800	-	-
Plan Cumulative	18.727	71.283	322.208	538.519	1,219.185	1,232.985	n/a	n/a
Cumulative % Allotment	10.30%	23.30%	13.15%	0.00%	0.00%	0.00%	0.00%	0.00%
Actual	1.929	12.248	32.987	-	-	-	-	-

1. Total of all FY09 appropriations, actual and planned obligations, and actual and planned expenditures

EBSP Program Initiatives

Description of Initiative I – Program Operations and Management

- Description: The Program Operations and Management initiative is broken down into five sections.
 1. Operations and Compliance/Interim Solutions
 - Moves, Adds and Changes \$15.35 million
 - Equipment Warehousing \$3.5 million
 2. Program Support
 - Program, Resource and Data Management Services \$26.0 million
 - Testing Services \$234 million
 - Audits, Travel, Training and Certification \$1.2 million

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

- 3. Engineering Support
 - Integration and Installation Management \$38.3 million
 - Engineering Technical and Design Support \$13.6 million
- 4. TSA Systems Integration Facility (TSIF) Support \$4.8 million
- 5. TSIF Building Purchase \$7.4 million
- 6. PC&B \$18.8 million
- Projected FY 2009 Obligations and Expenditures: \$97.5 million
- Projected ARRA Obligations and Expenditures: \$54.85 million

Description of Initiative II – **LOI** (FY 2009)

- Previously committed multiyear agreements for facility modifications
- Projected FY 2009 Obligations and Expenditures: \$200.0 million

Description of Initiative III – **EDS**

- FY 2009
 - The following EDSs will be purchased and installed:
 - Equipment for new terminals to permit TSA to screen bags on opening day to ensure that the airports do not rely on other screening solutions
 - Equipment necessary to maintain 100 percent screening compliance at existing installations
 - Equipment to fulfill existing TSA facility modification agreements (for example, EDS machines for LOI or Other Transactional Agreement (OTA) airports) for optimal in-line screening solutions that remove lobby congestion and decrease security concerns
 - Equipment to airports that have not received facility modifications funding but are proceeding with optimal system projects via their own financing, which are the most cost effective
 - Projected FY 2009 Obligations and Expenditures: \$146.6 million
 - Activities and Milestones: Installs based on airport schedules
- ARRA
 - Recapitalization efforts for airports with EDS solutions at the end of their life cycle
 - ETD-only airports that now require EDS technology to meet the screening requirements to improve screening effectiveness and to improve operational efficiencies through improved throughput and reduced on-the-job injuries
 - Projected ARRA Obligations and Expenditures: \$94.2 million
 - Activities and Milestones: Purchases to occur in Q3 FY 2009; installs based on airport schedules.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Description of Initiative IV – New Facility Modification Agreements to Construct a **Checked Baggage Inspection System (CBIS)**.

- FY 2009 – OTAs will be used to fund facility modifications to construct a CBIS at eight airports.
 - See Appendix M for Obligation data.
 - See Appendix O for Milestones.
 - Projected FY 2009 Obligations and Expenditures: \$67.32 million
- ARRA – OTAs will be used to fund facility modifications to construct a CBIS at 25 airports. TSA will assess the ability to add projects after completion of the cost validation for these 25 airports, which provides the anticipated cost difference between airport request funds and TSA-awarded funds.
 - See Appendix N for Obligation data.
 - See Appendix P for Milestones.
 - Projected ARRA Obligations and Expenditures: \$499.2 million

Description of Initiative V – Technology/Engineering Initiatives

- FY 2009 – Contracting Officer's Technical Representative/Engineering Initiatives will address:
 - Design and configuration changes/modifications (includes reconfiguration).
 - Requirements and Engineering Change Proposals.
 - Change in government guidance/objectives to improve efficiencies and equipment performance, such as employing equipment upgrades across the entire fleet of EDS (example: performance upgrade all CT-80 to CT-80DR) and implementing local networking at sites with multiple CT-80/CT-80DR systems to improve data collection efficiencies.
 - Non-operational issues, such as problems with repairs associated with equipment redeployment and out-of warranty.
 - Lack of commonality among checked baggage screening solutions.
 - Limitations on deployment of screening solutions based on existing site conditions.
 - Variances in technology capabilities that limit TSA flexibility in providing optimal screening solutions.
 - Projected Obligations and Expenditures: Total FY09 Engineering Initiatives: \$17.6 million
- ASP will address:
 - Remote visibility into the baggage resolution and screening areas in case of emergency to aid in threat identification and response.
 - A means to create an overall situational awareness to support oversight control for loss prevention, remote supervision, training, staffing, performance evaluation and legal or investigative needs with recordation.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

- An additional layer of security for the locations where TSA screens checked baggage to reduce the risk of threats from being introduced into checked baggage.
 - Projected Obligations and Expenditures: Total FY 2009 ASP Initiatives: \$5.0 million
 - Projected Obligations and Expenditures: Total ARRA ASP Initiatives: \$40.6 million
- Security Technology Integrated Program (STIP) will address:
 - Equipment in-service upgrades and automated data retrieval on equipment and screener performance to increase equipment availability, reliability and effectiveness; improve performance management and reduce overall operating and support costs.
 - Equipment replacement, reconfiguration and deployment strategies to increase throughput, systems capacity and effectiveness.
 - Projected Obligations and Expenditures: Total FY 2009 STIP Initiatives: \$8.0 million
- OI will address:
 - System integration and equipment purchases required for operational test and evaluation activities.
 - Projected Obligations and Expenditures: Total FY 2009 OI Initiatives: \$2.0 million
- Projected Obligations and Expenditures: Total FY 2009 Technology/Engineering Initiatives: \$32.6 millions
- Projected Obligations and Expenditures: Total ARRA Technology/Engineering Initiatives: \$40.6 millions

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

IV. Appendices

Appendix A. Abbreviations/Acronyms

ARRA	American Recovery and Reinvestment Act of 2009
AIT	Advanced Imaging Technology
ASP	Advanced Surveillance Program
AT	Advanced Technology
ATSA	Aviation & Transportation Security Act
BAO	Bomb Appraisal Officer
BLS	Bottled Liquids Scanner
CAD	Chemical Analyzer Detector
CAT/BPSS	Credential Authentication Technology/Boarding Pass Scanning Systems
CBIS	Checked Baggage Inspection System
DHS	Department of Homeland Security
EBSP	Electronic Baggage Screening Program
EDS	Explosives Detection Systems
EMD	Enhanced Metal Detector
ETD	Explosives Trace Detection
FAA	Federal Aviation Administration
FOC	Full Operational Capability
FY	Fiscal Year
HSA	Homeland Security Act of 2002
IOC	Initial Operational Capability
LOI	Letter of Intent
Next Gen ETD	Next Generation Explosives Trace Detector
OI	Operational Integration
OT&E	Operational Testing and Evaluation
OTA	Other Transactional Agreement
PC&B	Personnel Compensation and Benefits
PPA	Program, Project and Activity
PSP	Passenger Screening Program
QT&E	Qualification Testing and Evaluation
STIP	Security Technology Integration Program

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix A. Abbreviations/Acronyms (continued)

TIP	Threat Image Projection
TRX	Threat Image Projection (TIP) Ready X-Ray
TSA	Transportation Security Administration
TSIF	TSA Systems Integration Facility
TSO	Transportation Security Officer
UCS	Universal Conveyor Systems

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix B. Airport Codes

Airport Code	Airport Name	Airport Location
ACK	Nantucket Memorial	Nantucket, MA
AMA	Rick Husband Amarillo International	Amarillo, TX
ASE	Aspen-Pitkin County/Sardy Field	Aspen, CO
ATL	Hartsfield - Jackson Atlanta International	Atlanta, GA
BOI	Boise Air Terminal/Gowen Field	Boise, ID
BZN	Gallatin Field	Bozeman, MT
CHA	Lovell Field	Chattanooga, TN
CHS	Charleston AFB/International	Charleston, SC
CLT	Charlotte/Douglas International	Charlotte, NC
CMH	Port Columbus International	Columbus, OH
CMI	University of Illinois – Willard	Savoy, IL
COD	Yellowstone Regional	Cody, WY
COS	Colorado Springs	Colorado Springs, CO
CVG	Cincinnati/Northern Kentucky International	Covington, KY
DAY	James M Cox Dayton International	Dayton, OH
DCA	Ronald Reagan Washington National	Washington, DC
EGE	Eagle County Regional	Eagle, CO
EWR	Newark Liberty International	Newark, NJ
FAT	Fresno Yosemite International	Fresno, CA
GEG	Spokane International	Spokane, WA
GPI	Glacier Park International	Kalispell, MT
GRR	Gerald R. Ford International	Grand Rapids, MI
GUC	Gunnison-Crested Butte Regional	Gunnison, CO
HDN	Yampa Valley	Hayden, CO
HLN	Helena Regional	Helena, MT
HNL	Honolulu International	Honolulu, HI
HOU	William P. Hobby	Houston, TX
HSV	Huntsville International - Carl T Jones Field	Huntsville, AL
IAD	Washington Dulles International	Washington, DC
IAH	George Bush Intercontinental/Houston	Houston, TX

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix B. Airport Codes (continued)

Airport Code	Airport Name	Airport Location
ICT	Wichita Mid-Continent	Wichita, KS
ITO	Hilo International	Hilo, HI
JAC	Jackson Hole	Jackson Hole, WY
JFK	John F. Kennedy International	New York, NY
LGA	La Guardia	New York, NY
LIT	Little Rock National	Little Rock, AR
LSE	La Crosse Municipal	La Crosse, WI
MCO	Orlando International	Orlando, FL
MFR	Rogue Valley International – Medford	Medford, OR
MIA	Miami International	Miami, FL
MKK	Molokai Airport	Kaunakakai, HI
MSP	Minneapolis – St Paul International/Wold-Chamberlain	Minneapolis, MN
MSY	Louis Armstrong New Orleans International	New Orleans, LA
OAK	Metropolitan Oakland International	Oakland, CA
OGG	Kahului	Maui, HI
ORD	Chicago O’Hare International	Chicago, IL
PFN	Panama City-Bay County International	Panama City, FL
PHL	Philadelphia International	Philadelphia, PA
PHX	Phoenix Sky Harbor International Airport	Phoenix, AZ
PIE	St. Petersburg-Clearwater International	St. Petersburg, FL
PIT	Pittsburgh International	Pittsburgh, PA
PNS	Pensacola Regional	Pensacola, FL
PWM	Portland International Jetport	Portland, ME
RDM	Roberts Field	Redmond, OR
RDU	Raleigh-Durham International	Raleigh, NC
RNO	Reno/Tahoe International	Reno, NV
ROC	Greater Rochester International	Rochester, NY
SAN	San Diego International	San Diego, CA
SAT	San Antonio International	San Antonio, TX

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid “need-to-know” without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix B. Airport Codes (continued)

Airport Code	Airport Name	Airport Location
SBA	Santa Barbara Municipal	Santa Barbara, CA
SFO	San Francisco International	San Francisco, CA
SJC	Norman Y. Mineta San Jose International	San Jose, CA
SMF	Sacramento International	Sacramento, CA
SMX	Santa Maria Public Airport	Santa Maria, CA
SNA	John Wayne Airport-Orange County	Orange County, CA
STL	Lambert-Saint Louis International	St. Louis, MO
SUN	Friedman Memorial	Hailey, ID
TLH	Tallahassee Regional	Tallahassee, FL
TRI	Tri-Cities Regional	Bristol/Johnson/Kingsport, TN
TUL	Tulsa International	Tulsa, OK
TUS	Tucson International	Tucson, AZ
UTA	Tunica Municipal	Tunica, MS

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix C. Passenger Screening Program (PSP) Deployments by Airport

The number of procurements may not equal the number of deployments in one fiscal year. Planned airports are a function of the quantity and timing of units procured previously and the quantity of deployments being achieved. The chart below accounts for all deployments scheduled to occur by September 30, 2009.

Airport	SIZE	Planned ETD	Actual ETD	Planned AT	Actual AT	Planned AIT	Actual AIT	Planned BLS	Actual BLS	Planned CAT	Actual CAT	Planned Tech Cost	Actual Tech Cost	Planned Set Up Cost	Actual Set Up Cost
JFK	X	22		10	29			23		35		\$ 4,220,000	\$ 1,902,110	\$ 572,089	\$ 874,582
LAX	X	14			3			29				\$ 1,927,500	\$ 196,770	\$ 119,257	\$ 90,474
DCA	X	3					2	6				\$ 405,000	\$ 308,394	\$ 25,098	\$ 90,642
BWI	X	8			1			8		14		\$ 1,095,000	\$ 172,238	\$ 102,364	\$ 30,158
IAD	X	4			6			9				\$ 577,500	\$ 1,033,428	\$ 35,597	\$ 180,948
ORD	X	13		51	51	2		19				\$ 8,189,500	\$ 3,345,090	\$ 1,722,527	\$ 1,538,058
MIA	X	6			13			10				\$ 735,000	\$ 2,239,094	\$ 45,930	\$ 392,054
LGA	X	3		9	9			9				\$ 1,642,500	\$ 1,550,142	\$ 302,919	\$ 271,422
EWB	X	15		12	1	3		12				\$ 3,333,000	\$ 65,590	\$ 584,955	\$ 30,158
IAH	X	12		11	11			11				\$ 2,507,500	\$ 721,490	\$ 404,401	\$ 331,738
BOS	X	9		16	13	6		16				\$ 4,106,000	\$ 2,239,094	\$ 825,482	\$ 392,054
PHL	X	2		14	21			9				\$ 2,207,500	\$ 1,377,390	\$ 449,609	\$ 633,318
DTW	X	19		34	18			12				\$ 5,840,000	\$ 3,100,284	\$ 1,128,868	\$ 542,844
DFW	X	13			8			22				\$ 1,605,000	\$ 1,377,904	\$ 100,226	\$ 241,264
ATL	X	15			18		3	11				\$ 1,312,500	\$ 1,643,211	\$ 84,963	\$ 678,807
SFO	X	12		14	10		1	14				\$ 2,995,000	\$ 1,876,577	\$ 501,274	\$ 346,901
MSP	X	9		10	10			10				\$ 2,165,000	\$ 655,900	\$ 359,810	\$ 301,580
MCO	X	3		10	9			10				\$ 1,805,000	\$ 1,550,142	\$ 335,210	\$ 271,422
HNL	X	9		9	9			9				\$ 2,002,500	\$ 1,550,142	\$ 327,519	\$ 271,422
DEN	X	4						7				\$ 502,500	\$ -	\$ 31,331	\$ -
SJU	X	8		6	4			6				\$ 1,455,000	\$ 262,360	\$ 226,546	\$ 120,632
LAS	X	1						12				\$ 510,000	\$ -	\$ 29,696	\$ -
SEA	X	7		9	10			9				\$ 1,882,500	\$ 655,900	\$ 319,319	\$ 301,580
CLT	X	3		5	4			5				\$ 992,500	\$ 262,360	\$ 173,755	\$ 120,632
SAN	I	4		8	7			8				\$ 1,540,000	\$ 459,130	\$ 274,728	\$ 211,106
PHX	X	7			1			11				\$ 832,500	\$ 65,590	\$ 52,163	\$ 30,158
FLL	X	13		9	9			9				\$ 2,242,500	\$ 590,310	\$ 343,919	\$ 271,422
GUM	I			5				1				\$ 662,500	\$ -	\$ 152,923	\$ -
CVG	X	4		5	4			6				\$ 1,090,000	\$ 688,952	\$ 179,988	\$ 120,632
RDU	I	1		5	5			5				\$ 872,500	\$ 327,950	\$ 165,555	\$ 150,790

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix C. PSP Deployments by Airport (continued)

Airport	SIZE	Planned ETD	Actual ETD	Planned AT	Actual AT	Planned AIT	Actual AIT	Planned BLS	Actual BLS	Planned CAT	Actual CAT	Planned Tech Cost	Actual Tech Cost	Planned Set Up Cost	Actual Set Up Cost
PDX	I	3		6	5			6				\$ 1,155,000	\$ 861,190	\$ 206,046	\$ 150,790
MEM	I	4		4				5				\$ 927,500	\$ -	\$ 147,697	\$ -
STL	X	3		6	5			6				\$ 1,155,000	\$ 327,950	\$ 206,046	\$ 150,790
JAX	I	4		2	2		1	2				\$ 565,000	\$ 498,673	\$ 80,982	\$ 105,637
ANC	I			3	3			3				\$ 487,500	\$ 196,770	\$ 96,873	\$ 90,474
SYR	II			3				3				\$ 487,500	\$ -	\$ 96,873	\$ -
SJC	I	2		6	2			6				\$ 1,095,000	\$ 344,476	\$ 201,946	\$ 60,316
SLC	I			6	5		1	6				\$ 975,000	\$ 1,015,387	\$ 193,746	\$ 196,111
BUF	I			2	3			2				\$ 325,000	\$ 516,714	\$ 64,582	\$ 90,474
BNA	I	5		4				4				\$ 950,000	\$ -	\$ 149,664	\$ -
SAT	I	4		3	3			3				\$ 727,500	\$ 196,770	\$ 113,273	\$ 90,474
PIT	I			4	4			4				\$ 650,000	\$ 262,360	\$ 129,164	\$ 120,632
IND	IV				1			5				\$ 187,500	\$ 65,590	\$ 10,665	\$ 30,158
GSN	II			2	3			1				\$ 287,500	\$ 196,770	\$ 62,449	\$ 90,474
TPA	I	1		7	6		2	7				\$ 1,197,500	\$ 1,341,822	\$ 230,137	\$ 271,590
PBI	I	1		4				4				\$ 710,000	\$ -	\$ 133,264	\$ -
ONT	I	1		2				2				\$ 385,000	\$ -	\$ 68,682	\$ -
MKE	I	2		4	4			4				\$ 770,000	\$ 688,952	\$ 137,364	\$ 120,632
MDW	I			5	5							\$ 625,000	\$ 861,190	\$ 150,790	\$ 150,790
MCI	I	1		10	11							\$ 1,310,000	\$ 1,894,618	\$ 305,680	\$ 331,738
HOU	I			6								\$ 750,000	\$ -	\$ 180,948	\$ -
DAL	I	1		2	3							\$ 310,000	\$ 516,714	\$ 64,416	\$ 90,474
CLE	I	4		5	4							\$ 865,000	\$ 688,952	\$ 167,190	\$ 120,632
BUR	I	1		2	2							\$ 310,000	\$ 344,476	\$ 64,416	\$ 60,316
BHM	I			2								\$ 250,000	\$ -	\$ 60,316	\$ -
BDL	I			3	3							\$ 375,000	\$ 516,714	\$ 90,474	\$ 90,474
TUS	I	1		6	2							\$ 810,000	\$ 131,180	\$ 185,048	\$ 60,316
SNA	I	1		4	4							\$ 560,000	\$ 262,360	\$ 124,732	\$ 120,632
SFB	II	1		3	2							\$ 435,000	\$ 344,476	\$ 94,574	\$ 60,316
PVD	I	2		2	2							\$ 370,000	\$ 344,476	\$ 68,516	\$ 60,316

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix C. PSP Deployments by Airport (continued)

Airport	SIZE	Planned ETD	Actual ETD	Planned AT	Actual AT	Planned AIT	Actual AIT	Planned BLS	Actual BLS	Planned CAT	Actual CAT
ORF	I	1		2	2						
MSY	I	1		4							
GEG	I			2	2						
DAY	I			6							
ROC	II			6	2						
SMF	I	1		9	5						
RSW	I	1		4							
RNO	I	2		2	1						
OMA	I			2	2						
OKC	I			2	2						
OGG	I	2		6	2						
OAK	I			4	4						
AUS	I	2		4	2						
CMH	I	1		3							
STT	II	1		6	6						
MHT	I	1		3	3						
MDT	II	1		3							
LIH	I	2		3	4						
LGB	I			2	4						
FAI	II			2	2						
STX	III	1		3	3						
PPG	III	4		1	1						
FAT	II			2	2						
KOA	I	1		3	4						
GRR	II			4	2						
MLB	II			2							
DAB	II			2							
HPN	II			2							
ABE	II			2	2						
RIC	I	1		6	2		1				

Planned Tech Cost	Actual Tech Cost	Planned Set Up Cost	Actual Set Up Cost
\$ 310,000	\$ 344,476	\$ 64,416	\$ 60,316
\$ 560,000	\$ -	\$ 124,732	\$ -
\$ 250,000	\$ 344,476	\$ 60,316	\$ 60,316
\$ 750,000	\$ -	\$ 180,948	\$ -
\$ 750,000	\$ 344,476	\$ 180,948	\$ 60,316
\$ 1,185,000	\$ 861,190	\$ 275,522	\$ 150,790
\$ 560,000	\$ -	\$ 124,732	\$ -
\$ 370,000	\$ 172,238	\$ 68,516	\$ 30,158
\$ 250,000	\$ 344,476	\$ 60,316	\$ 60,316
\$ 250,000	\$ 344,476	\$ 60,316	\$ 60,316
\$ 870,000	\$ 131,180	\$ 189,148	\$ 60,316
\$ 500,000	\$ 688,952	\$ 120,632	\$ 120,632
\$ 620,000	\$ 131,180	\$ 128,832	\$ 60,316
\$ 435,000	\$ -	\$ 94,574	\$ -
\$ 810,000	\$ 393,540	\$ 185,048	\$ 180,948
\$ 435,000	\$ 516,714	\$ 94,574	\$ 90,474
\$ 435,000	\$ -	\$ 94,574	\$ -
\$ 495,000	\$ 262,360	\$ 98,674	\$ 120,632
\$ 250,000	\$ 262,360	\$ 60,316	\$ 120,632
\$ 250,000	\$ 131,180	\$ 60,316	\$ 60,316
\$ 435,000	\$ 196,770	\$ 94,574	\$ 90,474
\$ 365,000	\$ 65,590	\$ 46,558	\$ 30,158
\$ 250,000	\$ 131,180	\$ 60,316	\$ 60,316
\$ 435,000	\$ 262,360	\$ 94,574	\$ 120,632
\$ 500,000	\$ 344,476	\$ 120,632	\$ 60,316
\$ 250,000	\$ -	\$ 60,316	\$ -
\$ 250,000	\$ -	\$ 60,316	\$ -
\$ 250,000	\$ -	\$ 60,316	\$ -
\$ 250,000	\$ 131,180	\$ 60,316	\$ 60,316
\$ 810,000	\$ 285,377	\$ 185,048	\$ 105,637

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix C. PSP Deployments by Airport (continued)

Airport	SIZE	Planned ETD	Actual ETD	Planned AT	Actual AT	Planned AIT	Actual AIT	Planned BLS	Actual BLS	Planned CAT	Actual CAT	Planned Tech Cost	Actual Tech Cost	Planned Set Up Cost	Actual Set Up Cost
ABQ	I	2										\$ 120,000	\$ -	\$ 8,200	\$ -
ABI	III	1										\$ 60,000	\$ -	\$ 4,100	\$ -
AMA	II	1										\$ 60,000	\$ -	\$ 4,100	\$ -
BLI	III	2										\$ 120,000	\$ -	\$ 8,200	\$ -
BMI	III	3										\$ 180,000	\$ -	\$ 12,300	\$ -
BTX	II	1										\$ 60,000	\$ -	\$ 4,100	\$ -
CEF	III	1										\$ 60,000	\$ -	\$ 4,100	\$ -
CHO	III	1										\$ 60,000	\$ -	\$ 4,100	\$ -
CID	II	1										\$ 60,000	\$ -	\$ 4,100	\$ -
ELP	I	3										\$ 180,000	\$ -	\$ 12,300	\$ -
ERI	III	1										\$ 60,000	\$ -	\$ 4,100	\$ -
GSO	I	1										\$ 60,000	\$ -	\$ 4,100	\$ -
GSP	II	1										\$ 60,000	\$ -	\$ 4,100	\$ -
ILM	II	1										\$ 60,000	\$ -	\$ 4,100	\$ -
ITO	II	1										\$ 60,000	\$ -	\$ 4,100	\$ -
IWA	III	1										\$ 60,000	\$ -	\$ 4,100	\$ -
LEX	II	2										\$ 120,000	\$ -	\$ 8,200	\$ -
LNK	III	1										\$ 60,000	\$ -	\$ 4,100	\$ -
MBS	III	1										\$ 60,000	\$ -	\$ 4,100	\$ -
MGM	III	1										\$ 60,000	\$ -	\$ 4,100	\$ -
MYR	II	1										\$ 60,000	\$ -	\$ 4,100	\$ -
PIE	II	1										\$ 60,000	\$ -	\$ 4,100	\$ -
PNS	II	1										\$ 60,000	\$ -	\$ 4,100	\$ -
PSE	III	2										\$ 120,000	\$ -	\$ 8,200	\$ -
SBN	II	1										\$ 60,000	\$ -	\$ 4,100	\$ -
SPS	III	1										\$ 60,000	\$ -	\$ 4,100	\$ -
VLD	III	1										\$ 60,000	\$ -	\$ 4,100	\$ -
UNV	IV	2										\$ 120,000	\$ -	\$ 8,200	\$ -
BPT	IV	1										\$ 60,000	\$ -	\$ 4,100	\$ -
TUL	IV	N/A		N/A		N/A	1	N/A		N/A		\$ -	\$ 154,197	\$ -	\$ 45,321
TOTAL		346	0	472	427	11	12	401	0	49	0	\$ 97,671,000	\$ 49,480,526	\$17,190,790	\$13,421,318

*TUL was included as a new airport in the first quarter and second quarter expenditure plans. The "N/A" identified it as new airport, which meant there was no initial plan to compare the actual plan to.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix D. PSP FY 2009 Summary Spend Plan

Technology	Initial # of Units	Revised # of Units	Approved FY09 Funds	Revised FY09 Funds
Advanced Technology *	436	488	\$54.50	\$61.00
Universal Conveyor Systems	200	0	\$25.00	\$0.00
Advanced Imaging Technology	175	175	\$28.90	\$28.90
Credential Authentication Technology *	288	0	\$6.50	\$0.00
Bottled Liquids Scanners *	200	600	\$7.50	\$22.70
Explosives Trace Detectors	100	0	\$6.00	\$0.50
Subtotal			\$128.40	\$113.10
* Equipment quantities to be purchased with Fiscal Year 2009 funds and carryover funds were reallocated for Advanced Technology, Bottled Liquids Scanners, and Credential Authentication Technology.				
Program Operations and Management				
Integration			\$30.55	\$31.90
Warehouse			\$1.25	\$5.30
Engineering Support			\$4.10	\$7.70
Testing (IV&V)			\$3.30	\$0.05
Data Collection			\$3.00	\$0.00
TSA Systems Integration Facility (TSIF) Support			\$1.50	\$5.90
TSA Systems Integration Facility (TSIF) building purchase			\$0.00	\$2.40
Program and Data Management			\$12.20	\$9.30
Travel, Training, Supplies			\$1.10	\$0.95
Subtotal			\$57.00	\$63.50

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix D. PSP FY 2009 Summary Spend Plan (continued)

	Approved FY09 Funds	Revised FY09 Funds
Technical and Engineering Initiatives		
Security Technology Integration Program	\$7.60	\$10.50
Operational Integration of Emerging Technology	\$7.00	\$10.00
Threat Image Projection	\$4.00	\$4.00
Engineering Changes	\$2.40	\$0.50
Exit Lanes Data Collection	\$1.60	\$1.60
Subtotal	\$22.60	\$26.60
Safety and Optimization		
Equipment	\$5.00	\$5.00
System Integrator	\$3.00	\$3.00
Engineering Support	\$2.50	\$2.50
Airport Projects	\$2.00	\$2.00
Project Logistics	\$1.00	\$1.00
Subtotal	\$13.50	\$13.50
Checkpoint Reconfiguration		
Ancillary Equipment	\$3.00	\$3.00
Glass Partitions	\$2.70	\$2.70
Checkpoint Optimizations	\$1.70	\$1.70
Divest/Composure/Roller Tables	\$1.50	\$1.50
Project Logistics	\$1.50	\$1.50
Engineering and Technical Support	\$1.00	\$1.00
Travel	\$0.10	\$0.10
Subtotal	\$11.50	\$11.50

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix D. PSP FY 2009 Summary Spend Plan (continued)

Advanced Surveillance Program	Approved FY09 Funds	Revised FY09 Funds
Boston (BOS)	\$4.30	\$1.80
Orlando (MCO)	\$3.30	\$0.00
Philadelphia (PHL)	\$1.60	\$3.40
Phoenix (PHX)	\$0.00	\$0.00
Atlanta (ATL)	\$0.00	\$0.00
Chicago (ORD)	\$0.80	\$0.80
Cleveland (CLE)	\$0.10	\$0.10
Louis Munoz Marin (SJU)	\$0.10	\$0.10
Long Beach (LGB)	N/A	\$0.30
Providence (PVD)	N/A	\$1.30
San Francisco	N/A	\$2.40
Program Support	\$0.80	\$0.80
Subtotal	\$11.00	\$11.00
Personnel Compensation and Benefits	\$6.00	\$6.00
Total*	\$250.00	\$245.20

*\$4.8 million was reallocated from the checkpoint support Program, Project and Activity.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix E. PSP American Recovery and Reinvestment Act (ARRA) Summary Spend Plan

Technology	Initial # of Units	Revised # of Units	Approved ARRA Funds	Revised ARRA Funds
Advanced Technology *	755	611	\$94.40	\$76.40
Universal Conveyor Systems	275	228	\$34.40	\$28.50
Advanced Imaging Technology	200	200	\$32.20	\$32.20
Credential Authentication Technology	0	800	\$0.00	\$18.00
Bottled Liquids Scanners	500	500	\$18.80	\$18.80
Explosives Trace Detectors	300	400	\$18.00	\$22.00
Chemical Analyzer Detectors	N/A	140	N/A	\$7.00
Subtotal			\$197.80	\$202.90
* Reduced to add Credential Authentication Technology to ARRA spend plan.				
Program Operations and Management				
Integration			\$57.90	\$68.20
Testing (IV&V)			\$2.00	\$2.00
Program and Data Management			\$23.00	\$7.50
Subtotal			\$82.90	\$77.70
Technical and Engineering Initiatives				
Engineering Changes			\$9.90	\$9.90
Subtotal			\$9.90	\$9.90

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix E. PSP ARRA Summary Spend Plan (continued)

Advanced Surveillance Program	Approved ARRA Funds	Revised ARRA Funds
Ronald Reagan Washington National	\$0.60	\$1.90
Cincinnati/Northern Kentucky International	\$1.80	\$0.70
Spokane International	\$1.10	\$1.70
Metropolitan Oakland International	\$2.20	\$0.00
Boise Gowen Field Air Terminal	N/A	\$0.80
Kent County Airport	N/A	\$0.60
Washington Dulles International	N/A	\$2.60
Will Rogers World	N/A	\$0.70
Chicago Midway International	N/A	\$1.40
Eppley Airfield	N/A	\$0.70
James M Cox Dayton International Airport	N/A	\$0.45
Kansas City International	N/A	\$2.80
Adams Field	N/A	\$0.40
Tampa International	N/A	\$2.10
Subtotal	\$5.70	\$16.85
Personnel Compensation and Benefits	\$3.80	\$3.80
Total*	\$300.00	\$311.15

Numbers may not add due to rounding.

*Revised ARRA funds: \$11.1 million was shifted from Explosives Detection Systems to PSP for Advanced Surveillance Program/Closed Circuit Television projects.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix F. PSP FY 2009 Obligation Data

Spend Plan Categories	\$ in millions	Planned Obligation Date	\$ in millions	Revised Obligation Date
Advanced Technology	\$54.50	Jul-09	\$61.00	Nov-09
Universal Conveyor Systems	\$25.00	Aug-09	\$0.00	Mar-10
Advanced Imaging Technology	\$28.90	Jul-09	\$28.90	Dec-09
Credential Authentication Technology	\$6.50	Jul-09	\$0.00	Sep-09
Bottled Liquids Scanners	\$7.50	Jul-09	\$22.70	Sep-09
Explosives Trace Detectors	\$6.00	Jul-09	\$0.50	Sep-09
Integration	\$30.55	Jul-09	\$31.90	Sep-09
Program Operations and Management	\$26.45	Ongoing	\$31.60	Ongoing
Technical and Engineering Initiatives	\$22.60	Ongoing	\$26.60	Ongoing
Safety and Optimization	\$13.50	Ongoing	\$13.50	Ongoing
Checkpoint Reconfiguration	\$11.50	Ongoing	\$11.50	Ongoing
Advanced Surveillance Program	\$11.00	Ongoing	\$11.00	Ongoing
Personnel Compensation and Benefits	\$6.00	Ongoing	\$6.00	Ongoing
Subtotal	\$250.00		\$245.20	

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix G. PSP ARRA Obligation Data

Spend Plan Categories	\$ in millions	Planned Obligation Date	\$ in millions	Revised Obligation Date
Advanced Technology	\$94.40	Jul-09	\$76.40	May-09 Nov-09
Universal Conveyor Systems	\$34.40	Aug-09	\$28.50	Mar-10
Advanced Imaging Technology	\$32.20	Jul-09	\$32.20	Sep-09
Credential Authentication Technology	\$0.00	N/A	\$18.00	Sep-09
Bottled Liquids Scanners	\$18.80	Jul-09	\$18.80	Sep-09
Explosives Trace Detectors	\$18.00	Jul-09	\$22.00	Sep-09
Chemical Analyzer Detectors	N/A	N/A	\$7.00	Sep-09 Dec-09
Integration	\$57.90	Jul-09	\$68.20	Sep-09
Program Operations and Management	\$25.00	Ongoing	\$9.50	Ongoing
Technical and Engineering Initiatives	\$9.90	Ongoing	\$9.90	Ongoing
Advanced Surveillance Program	\$5.70	Ongoing	\$16.85	Ongoing
Personnel Compensation and Benefits	\$3.80	Ongoing	\$3.80	Ongoing
Subtotal	\$300.00		\$311.15	

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix H. PSP FY 2009 Milestones

Advanced Technology	Planned	Revised
Initial Qualified Data Package Down Select	Mar-09	Mar-09
Qualification Testing and Evaluation (QT&E) Begins	Mar-09	Aug-09
Operational Testing and Evaluation (OT&E) Begins	Apr-09	Aug-09
Contract Award	Jul-09	Nov-09
Advanced Imaging Technology		
QT&E Begins	Feb-09	Aug-09
OT&E Begins	Apr-09	Aug-09
Request for Proposals Released	Jun-09	Jun-09
Contract Award	Jul-09	Sep-09
Bottled Liquids Scanners		
QT&E Begins	Mar-09	Jun-09
OT&E Begins	Mar-09	Jul-09
Contract Award	Jul-09	Sep-09
Advanced Surveillance Program		
Boston Logan International	May-09	Sep-09
Philadelphia International	May-09	Sep-09
Orlando International	May-09	N/A
Phoenix Sky Harbor International	May-09	N/A
Chicago O'Hare International	N/A	Sep-09
Cleveland Hopkins International	N/A	Sep-09
Luis Munoz Marin International	N/A	Sep-09
Long Beach	N/A	Sep-09
Theodore Francis Green International	N/A	Sep-09
San Francisco International	N/A	Sep-09

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix I. PSP ARRA Milestones

Advanced Technology	Planned	Revised
Initial Qualified Data Package Down Select	Mar-09	Mar-09
Qualification Testing and Evaluation (QT&E) Begins	Mar-09	Aug-09
Operational Testing and Evaluation (OT&E) Begins	Apr-09	Aug-09
Contract Award	Jul-09	Nov-09
Universal Conveyor System		
QT&E Begins	TBD	TBD
OT&E Begins	TBD	TBD
Contract Award	TBD	Mar-10
Advanced Imaging Technology		
QT&E Begins	Feb-09	Aug-09
OT&E Begins	Apr-09	Aug-09
Request for Proposals Released	Jun-09	Jun-09
Contract Award	Jul-09	Sep-09
Credential Authentication Technology		
QT&E Begins	Aug-09	Aug-09
OT&E Begins	Aug-09	Aug-09
Contract Award	Sep-09	Sep-09
Bottled Liquids Scanners		
QT&E Begins	Mar-09	Jun-09
OT&E Begins	Mar-09	Jul-09
Contract Award	Jul-09	Sep-09
Next Gen Explosives Trace Detectors		
QT&E Began	Nov-07	Nov-07
OT&E Began	Mar-08	Mar-08
Contract Award	Aug-08	Aug-08

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix I. PSP ARRA Milestones (continued)

Advanced Surveillance Program	Planned	Revised
Ronald Reagan Washington National	Jun-09	Jun-09
Cincinnati/Northern Kentucky International	Jun-09	Jun-09
Spokane International	Jun-09	Jul-09
Metropolitan Oakland International	Jun-09	N/A
Boise Gowen Field Air Terminal	N/A	Jul-09
Kent County Airport	N/A	Jul-09
Washington Dulles International	N/A	Sep-09
Will Rogers World	N/A	Sep-09
Chicago Midway International	N/A	Sep-09
Eppley Airfield	N/A	Sep-09
James M Cox Dayton International	N/A	Sep-09
Kansas City International	N/A	Sep-09
Adams Field	N/A	Sep-09
Tampa International	N/A	Sep-09

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix J. PSP FY 2009 Actual vs. Anticipated Unobligated Balance, as of June 30, 2009

FY09	Anticipated			
Spend Plan Category (\$M)	Budgeted	Obligated	Unobligated	Unobligated at end of FY09
Checkpoint Technology	\$203.20	\$22.90	\$180.30	\$90.00
Checkpoint Reconfiguration	\$11.50	\$5.10	\$6.40	\$0.00
ASP	\$11.00	\$0.00	\$11.00	\$0.00
Safety Optimization	\$13.50	\$0.00	\$13.50	\$3.70
PC&B	\$6.00	\$3.80	\$2.20	\$1.15
Total	\$245.20	\$31.80	\$213.40	\$94.85

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix K. PSP ARRA Actual vs. Anticipated Unobligated Balance, as of June 30, 2009

ARRA Spend Plan Category (\$M)	Budgeted	Obligated	Unobligated	Anticipated Unobligated at end of FY09
Checkpoint Technology	\$290.50	\$2.90	\$287.60	\$138.30
Advanced Surveillance Program	\$16.85	\$2.50	\$14.35	\$0.00
Personnel Compensation and Benefits	\$3.80	\$0.00	\$3.80	\$3.80
Total	\$311.15	\$5.40	\$305.75	\$142.10

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix L. Electronic Baggage Screening Program (EBSP) FY 2009 Obligation by Project

Project	Spend Plan	Project Timelines				Project Cost		Obligation Schedule		Obligation Balances			Expenditures
		Ant. Start Date	Actual Start Date	Ant. End Date	Actual End Date	Initial Dollar Amt.	Revised Dollar Amt.	Planned Obligation	Actual Obligation	Obligated	Unobligated Balance	Anticipated Unobligated	
JFK	LOI	Sep-08	Sep-08	Sep-13	-	\$78.00	-	May-09	-	\$0.00	\$78.00	\$0.00	\$0.00
EWB	LOI	Sep-08	Sep-08	Sep-13	-	\$60.00	-	May-09	-	\$0.00	\$60.00	\$0.00	\$0.00
LGA	LOI	Sep-08	Sep-08	Sep-13	-	\$62.00	-	May-09	-	\$0.00	\$62.00	\$0.00	\$0.00
ORD	OTA	Aug-09	-	Feb-10	-	\$19.80	-	May-09	-	\$0.00	\$19.80	\$0.00	\$0.00
ICT	OTA	Dec-09	-	Mar-11	-	\$8.25	-	Sep-09	-	\$0.00	\$8.25	\$0.00	\$0.00
SNA	OTA	Sep-09	-	Dec-10	-	\$8.77	-	Sep-09	-	\$0.00	\$8.77	\$0.00	\$0.00
FAT	OTA	Sep-09	-	Jan-11	-	\$3.75	-	Jun-09	-	\$0.15	\$3.60	\$0.00	\$0.00
MSP	OTA	Nov-09	-	Apr-13	-	\$8.00	-	Sep-09	-	\$0.00	\$8.00	\$0.00	\$0.00
TRI	OTA	Jan-09	-	Sep-09	-	\$3.25	-	Sep-09	-	\$0.00	\$3.25	\$0.00	\$0.00
AMA	OTA	Mar-09	-	Jan-11	-	\$8.25	-	Sep-09	-	\$0.00	\$8.25	\$0.00	\$0.00
PFN	OTA	Jul-09	-	Mar-10	-	\$7.25	-	Jul-09	-	\$0.00	\$7.25	\$0.00	\$0.00
Medium Throughput EDS	Purchase	Mar-09	-	Sep-09	-	\$84.74	-	Mar-09	-	\$0.00	\$84.74	\$0.00	\$0.00
Reduced Size EDS	Purchase	Jan-09	Mar-09	Sep-09	-	\$23.00	-	Jan-09	Mar-09	\$19.52	\$3.48	\$0.00	\$13.38
EWB	Install	Oct-09	-	May-09	-	\$1.24	-	Oct-09	-	\$0.00	\$1.24	\$0.00	\$0.00
ORD	Install	Dec-09	-	Jun-09	-	\$1.55	-	Dec-09	-	\$0.00	\$1.55	\$0.00	\$0.00
CVG	Install	Aug-09	Mar-09	Mar-09	-	\$2.16	-	Aug-09	Mar-09	\$2.43	-\$0.27	\$0.00	\$0.23
MCO	Install	Aug-09	Apr-09	Mar-09	-	\$2.65	-	Aug-09	Mar-09	\$0.72	\$1.93	\$0.00	\$0.11
MIA	Install	Sep-09	Apr-09	Apr-09	-	\$2.63	-	Sep-09	Mar-09	\$1.12	\$1.51	\$0.00	\$0.00
IAH	Install	Dec-09	-	May-09	-	\$1.55	-	Dec-09	-	\$0.00	\$1.55	\$0.00	\$0.00
ACK	Install	Feb-09	-	Feb-09	-	\$0.12	-	Feb-09	-	\$0.02	\$0.10	\$0.00	\$0.00
SAT	Install	Oct-09	-	Aug-09	-	\$2.42	-	Oct-09	-	\$0.00	\$2.42	\$0.00	\$0.00
PFN	Install	Dec-09	-	Jun-09	-	\$0.92	-	Dec-09	-	\$0.00	\$0.92	\$0.00	\$0.00
SJC	Install	Jul-09 & Jan-10	-	Mar-10 & Sep-10	-	\$2.92	-	Jul-09	-	\$0.00	\$2.92	\$0.00	\$0.00
AMA	Install	May-09	-	May-09	-	\$0.82	-	May-09	-	\$0.00	\$0.82	\$0.00	\$0.00
MFR	Install	Feb-09	Feb-09	Feb-09	-	\$1.04	-	May-09	Feb-09	\$0.76	\$0.28	\$0.00	\$0.00
TLH	Install	Nov-09	-	Jun-09	-	\$1.03	-	Nov-09	-	\$0.00	\$1.03	\$0.00	\$0.00
OGG	Install	Aug-09	-	Mar-10	-	\$1.10	-	Aug-09	-	\$0.00	\$1.10	\$0.00	\$0.00

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix L. EBSP FY 2009 Obligation by Project (continued)

Project	Spend. Plan	Project Timelines				Project Cost		Obligation Schedule		Obligation Balances			Expenditures
		Ant. Start Date	Actual Start Date	Ant. End Date	Actual End Date	Initial Dollar Amt.	Revised Dollar Amt.	Planned Obligation	Actual Obligation	Obligated	Unobligated Balance	Anticipated Unobligated	
PHX	Install	Aug-09	-	Mar-09	-	\$0.45	-	Aug-09	-	\$0.00	\$0.45	\$0.00	\$0.00
PNS	Install	Jan-09	-	Mar-09	-	\$0.12	-	Jul-09	-	\$0.03	\$0.09	\$0.00	\$0.00
RDU	Install	Mar-09	-	Oct-09	-	\$0.00	-	Mar-09	-	\$0.00	\$0.00	\$0.00	\$0.00
RNO	Install	Jul-09	-	Jul-09	-	\$0.90	-	Aug-09	-	\$0.00	\$0.90	\$0.00	\$0.00
ROC	Install	May-09	-	May-09	-	\$0.00	-	May-09	-	\$0.00	\$0.00	\$0.00	\$0.00
SAN	Install	Aug-09	Mar-09	Mar-09	-	\$0.24	-	Aug-09	Feb-09	\$0.19	\$0.05	\$0.00	\$0.00
SFO	Install	Jan-09	-	Apr-09	-	\$1.43	-	Jan-09	-	\$0.00	\$1.43	\$0.00	\$0.00
SNA	Install	Nov-09	-	Jun-09	-	\$2.11	-	Nov-09	-	\$0.00	\$2.11	\$0.00	\$0.00
LSE	Install	May-09	-	May-09	-	\$0.08	-	May-09	-	\$0.00	\$0.08	\$0.00	\$0.00
PIT	Install	Aug-09	-	Aug-09	-	\$0.08	-	Aug-09	-	\$0.00	\$0.08	\$0.00	\$0.00
SMX	Install	Jun-09	-	Jun-09	-	\$0.08	-	Jun-09	-	\$0.00	\$0.08	\$0.00	\$0.00
ITO	Install	Jun-09	-	Jun-09	-	\$0.08	-	Jun-09	-	\$0.00	\$0.08	\$0.00	\$0.00
GPI	Install	Jun-09	-	Jun-09	-	\$0.08	-	Jun-09	-	\$0.00	\$0.08	\$0.00	\$0.00
MKK	Install	Jun-09	-	Jun-09	-	\$0.08	-	Jun-09	-	\$0.00	\$0.08	\$0.00	\$0.00
HLN	Install	Jun-09	-	Jun-09	-	\$0.08	-	Jun-09	-	\$0.00	\$0.08	\$0.00	\$0.00
CHA	Install	Mar-09	-	Mar-09	-	\$0.08	-	Mar-09	-	\$0.00	\$0.08	\$0.00	\$0.00
CHS	Install	Feb-09	-	Feb-09	-	\$0.26	-	Feb-09	-	\$0.00	\$0.26	\$0.00	\$0.00
CMI	Install	Apr-09	-	Apr-09	-	\$0.08	-	Apr-09	-	\$0.00	\$0.08	\$0.00	\$0.00
SUN	Install	Apr-09	-	Apr-09	-	\$0.08	-	Apr-09	-	\$0.01	\$0.07	\$0.00	\$0.00
GUC	Install	May-09	-	May-09	-	\$0.08	-	May-09	-	\$0.00	\$0.08	\$0.00	\$0.00
SAN-RS	Install	Apr-09	-	Apr-09	-	\$0.60	-	Apr-09	-	\$0.00	\$0.60	\$0.00	\$0.00
PHL-RS	Install	May-09	-	May-09	-	\$0.89	-	May-09	-	\$0.00	\$0.89	\$0.00	\$0.00
HDN	Install	May-09	-	May-09	-	\$1.24	-	May-09	-	\$0.00	\$1.24	\$0.00	\$0.00
EGE	Install	Jun-09	-	Jun-09	-	\$0.72	-	Jun-09	-	\$0.00	\$0.72	\$0.00	\$0.00
ASE**	Install	Replaced with SBA	-	Replaced with SBA	-	\$0.00	-	Project cancelled and replaced with SBA	-	\$0.00	\$0.00	\$0.00	\$0.00
SBA**	Install	Jul-09	-	Jul-09	-	\$0.72	-	Jul-09	-	\$0.00	\$0.72	\$0.00	\$0.00
TUS	Install	Mar-09	-	Mar-09	-	\$0.33	-	Mar-09	-	\$0.00	\$0.33	\$0.00	\$0.00
UTA	Install	Jun-09	-	Jun-09	-	\$0.08	-	Jun-09	-	\$0.01	\$0.07	\$0.00	\$0.00
RDM	Install	Feb-09	-	Feb-09	-	\$0.72	-	Feb-09	-	\$0.00	\$0.72	\$0.00	\$0.00
Recap	Install	Ongoing thru Sept	-	Sep-09	-	\$5.00	-	Ongoing thru Sept	-	\$0.00	\$5.00	\$0.00	\$0.00

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know", without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix L: EBSP FY 2009 Obligation by Project (continued)

Project	Spend Plan	Project Timelines				Project Cost		Obligation Schedule		Obligation Balances			Expenditures
		Ant. Start Date	Actual Start Date	Ant. End Date	Actual End Date	Initial Dollar Amt.	Revised Dollar Amt.	Planned Obligation	Actual Obligation	Obligated	Unobligated Balance	Anticipated Unobligated	
COTR/ Engineering Initiatives	T&E	Ongoing thru Sept	-	Sep-09	-	\$25.00	17.60	Ongoing thru Sept	n/a	\$2.07	\$15.53	\$3.80	0.00
STIP	T&E	Ongoing thru Sept	-	Sep-09	-	\$8.00	-	Ongoing thru Sept	n/a	\$1.03	\$6.97	\$0.00	0.00
ASP	T&E	Ongoing thru Sept	-	Sep-09	-	\$5.00	-	Ongoing thru Sept	n/a	\$0.00	\$5.00	\$0.00	0.00
OI	T&E	Ongoing thru Sept	-	Sep-09	-	\$2.00	-	Ongoing thru Sept	n/a	\$0.00	\$2.00	\$0.00	0.00
Ops & Compliance, Program Support, Engineering Support, TSIF Support, & PC&B	P,O & M	Ongoing thru Sept	-	Sep-09	-	\$74.90	90.08	Ongoing thru Sept	n/a	\$30.50	\$59.58	\$0.02	0.00
TSIF Building Purchase	P,O & M	Ongoing thru Sept	-	Sep-09	-	\$7.40		Ongoing thru Sept	n/a	\$0.00	\$0.00	\$0.00	0.00

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix M. EBSP ARRA Obligation by Project

Project	Spend. Plan	Project Timelines				Project Cost		Obligation Schedule		Obligation Balances			Expenditures
		Ant. Start Date	Actual Start Date	Ant. End Date	Actual End Date	Initial Dollar Amt.	Revised Dollar Amt.	Planned Obligation	Actual Obligation	Obligated	Unobligated Balance	Anticipated Unobligated	
HNL	OTA	Jul-09	-	Aug-10	-	\$43.50	\$24.50	Jul-09	-	\$0.00	\$24.50	\$0.00	-
OGG	OTA	Aug-09	-	Nov-10	-	\$18.50	\$7.20	Aug-09	-	\$0.00	\$7.20	\$0.00	-
PHL	OTA	Jun-09	-	Aug-10	-	\$53.00	\$26.60	Jun-09	Jun-09	\$26.60	\$0.00	\$0.00	-
SJC	OTA	Sep-09	-	Dec-10	-	\$31.00	\$23.94	Sep-09	-	\$0.00	\$23.94	\$0.00	-
TLH	OTA	-	-	-	-	\$15.00	-	-	-	-	-	-	-
PWM	OTA	Aug-09	-	Nov-10	-	\$13.30	\$13.50	Aug-09	-	\$0.00	\$13.50	\$0.00	-
SFO	OTA	Jun-09	-	Aug-10	-	\$30.00	\$15.35	Jun-09	Jul-09	\$15.35	\$0.00	\$0.00	-
SMF	OTA	Jul-09	-	Aug-10	-	\$53.00	\$11.34	Jul-09	-	\$0.00	\$11.34	\$0.00	-
JAC	OTA	Jun-09	-	Aug-10	-	\$8.80	\$6.21	Jun-09	Jun-09	\$6.21	\$0.00	\$0.00	-
HSV	OTA	Sep-09	-	Dec-10	-	\$27.50	\$1.50	Sep-09	-	\$0.00	\$1.50	\$0.00	-
MCO	OTA	Jul-09	-	Aug-10	-	\$104.50	\$14.93	Jul-09	Jul-09	\$14.93	\$0.00	\$0.00	-
MCO	OTA	Sep-09	-	Dec-10	-	-	\$13.80	Sep-09	-	\$0.00	\$13.80	\$0.00	-
SAT	OTA	Nov-09	-	Dec-11	-	\$14.39	\$0.00	Sep-09	-	\$0.00	\$14.39	\$0.00	-
DAY	OTA	Aug-09	-	Nov-10	-	\$20.00	\$9.70	Aug-09	-	\$0.00	\$9.70	\$0.00	-
ATL	OTA	Sep-09	-	Dec-10	-	\$54.20	\$21.20	Sep-09	-	\$0.00	\$21.20	\$0.00	-
MSY	OTA	Dec-09	-	Apr-11	-	\$14.50	\$24.97	Dec-09	-	\$0.00	\$24.97	\$0.00	-
CMH	OTA	Sep-09	-	Dec-10	-	\$60.00	\$26.50	Sep-09	-	\$0.00	\$26.50	\$0.00	-
STL	OTA	Sep-09	-	Dec-10	-	\$0.00	\$31.50	Sep-09	-	\$0.00	\$31.50	\$0.00	-
IAD	OTA	Sep-09	-	Dec-10	-	\$0.00	\$148.91	Sep-09	-	\$0.00	\$148.91	\$0.00	-
COD	OTA	Sep-09	-	Dec-10	-	\$0.00	\$0.35	Sep-09	-	\$0.00	\$0.35	\$0.00	-
HOU	OTA	Sep-09	-	Dec-10	-	\$0.00	\$0.51	Sep-09	-	\$0.00	\$0.51	\$0.00	-
PIE	OTA	Oct-09	-	Jan-11	-	\$0.00	\$0.63	9-Oct	-	\$0.00	\$0.63	\$0.00	-
BZN	OTA	Dec-09	-	Apr-11	-	\$0.00	\$6.80	Dec-09	-	\$0.00	\$6.80	\$0.00	-
TUL	OTA	Dec-09	-	Mar-11	-	\$0.00	\$4.72	Dec-09	-	\$0.00	\$4.72	\$0.00	-
CLT	OTA	Jan-09	-	Mar-11	-	\$0.00	\$33.78	Jan-09	-	\$0.00	\$33.78	\$0.00	-
COS	OTA	Jan-09	-	Mar-11	-	\$0.00	\$7.41	Jan-09	-	\$0.00	\$7.41	\$0.00	-
LIT	OTA	Nov-09	-	Feb-11	-	\$0.00	\$8.96	Nov-09	-	\$0.00	\$8.96	\$0.00	-
Reduced Sized EDS	Purchase	Ongoing thru Sept	May-09	Sep-09	-	\$64.20	\$94.20	Ongoing thru Sept	n/a	\$47.50	\$46.70	\$0.00	\$17.50
ASP	T&E	Ongoing thru Sept	-	Sep-09	-	\$2.20	\$40.60	Ongoing thru Sept	n/a	\$1.40	\$39.20	\$0.00	\$1.40
Ops & Compliance, Program Support, Engineering Support, TSIF Support, & PC&B	P,O & M	Ongoing thru Sept	-	Sep-09	-	\$32.00	\$54.85	Ongoing thru Sept	n/a	\$0.00	\$54.85	\$0.00	-

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix N. EBSP FY 2009 Summary Spend Plan

Summary

Section	\$ in Millions
Program Operations and Management	\$97.5
Letters of Intent (LOI)	\$200.0
Other Transaction Agreement (OTA) – New Facility Modification Agreement Projects	\$67.3
Explosives Detection Systems (EDS) Purchase and Install	\$146.6
Technology/Engineering Initiatives	\$32.6
Total	\$544.0

Program Operations and Management

Project Description	Total TSA FY09 Project Cost
Operations and Compliance/Interim Solutions	
- Moves, Adds and Changes	\$7.5
- Equipment Warehousing	\$3.5
Program Support	
- Program, Resource and Data Management Services	\$16.0
- Testing Services	\$18.1
- Audits, Travel, Training and Certification	\$1.2
Engineering Support	
- Integration and Installation Management	\$13.5

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix N. EBSP FY 2009 Summary Spend Plan (continued)

Project Description	Total TSA FY 2009 Project Cost
-Engineering Technical and Design Support	\$10.5
TSA Systems Integration Facility (TSIF) Support	\$4.8
TSIF Building Purchase	\$7.4
Personnel Compensation and Benefits	\$15.0
Total	\$97.5

LOI Projects

Airport	Scope of Work	TSA Cost Share	Total TSA FY 2009 Project Cost
JFK	LOI funding for the airport to construct a Checked Baggage Inspection System (CBIS) for Terminals 2, 3, 4 and 7	90%	\$78.0
EWR	LOI funding for the airport to construct a CBIS for Terminals A, B and C	90%	\$60.0
LGA	LOI funding for the airport to construct a CBIS for Terminals USAir and Central Terminal Building	90%	\$62.0
Total LOI Projects			\$200.0

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix N. EBSP FY 2009 Summary Spend Plan (continued)

OTA – New Facility Modification Agreement Projects

Airport	Scope of Work	TSA Cost Share*	Total TSA FY09 Project Cost
ORD	OTA funding for the airport to construct a CBIS for Terminal 1-B South	90%	\$19.8
ICT	OTA funding for the airport to construct a CBIS for Terminal Main	95%	\$8.25
SAT	OTA funding for the airport to construct a CBIS for Terminal 1/B (funded via American Recovery and Reinvestment Act)	90%	\$0.0
FAT	OTA funding for the airport to construct a CBIS for Terminal Main	95%	\$3.75
MSP	OTA funding for the airport to construct a CBIS for the Lindbergh Terminal	90%	\$8.0
TRI	OTA funding for the airport to construct a CBIS for Terminal Main	95%	\$3.25
AMA	OTA funding for the airport to construct a CBIS for Terminal Main	95%	\$8.25
PFN	OTA funding for the airport to construct a CBIS for New Terminal	95%	\$7.25
SNA	OTA funding for the airport to construct a CBIS for Terminals A and B	90%	\$8.77
Total OTA			\$67.3

* TSA's cost share in this table is 90 percent for a project at a medium or large hub airport and 95 percent for a project at a small and non-hub airport.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix N. EBSP FY 2009 Summary Spend Plan (continued)

FY 2009 EDS Purchase and Install Projects

Airport	Scope of Work	Purchase	Deployment	TSA Cost Share*	Total TSA FY 2009 Project Cost
EWR	Purchase, install, integrate, network and test (3) Medium Speed EDS	\$3.24	\$1.24	100%	\$4.48
ORD	Purchase, install, integrate, network and test (4) Medium Speed EDS for Terminal 1 B-South	\$4.32	\$1.55	100%	\$5.87
CVG	Purchase, install, integrate, network and test(5) Medium Speed EDS for Terminal 3	\$5.40	\$2.16	100%	\$7.56
MCO	Purchase, install, integrate, network and test (7) Medium Speed EDS for Terminal Central East	\$7.56	\$2.65	100%	\$10.21
MIA	Purchase, install, integrate, network and test (8) Medium Speed EDS for Terminal East/Cruise Matrix	\$8.64	\$2.63	100%	\$11.27
IAH	Purchase, install, integrate, network and test (4) Medium Speed EDS for Terminal D	\$4.32	\$1.55	100%	\$5.87
ACK	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.42	\$0.12	100%	\$0.54
SAT	Purchase, install, integrate, network and test (7) Medium Speed EDS for Terminal 1/B	\$7.56	\$2.42	100%	\$9.98
PFN	Purchase, install, integrate, network and test (2) Medium Speed EDS for Terminal New	\$2.16	\$0.92	100%	\$3.08

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix N. EBSP FY 2009 Summary Spend Plan (continued)

Airport	Scope of Work	Purchase	Deployment	TSA Cost Share*	Total TSA FY 2009 Project Cost
SJC	Purchase, install, integrate, network and test (8) Medium Speed EDS for Terminal A/B	\$9.72	\$2.92	100%	\$12.64
AMA	Purchase, install, integrate, network and test (2) Reduced Size EDS for Terminal Main	\$0.84	\$0.82	100%	\$1.66
MFR	Purchase, install, integrate, network and test (2) Reduced Size EDS for Terminal Main	\$0.84	\$1.04	100%	\$1.88
TLH	Purchase, install, integrate, network and test (2) Medium Speed EDS for Terminal Main	\$2.16	\$1.03	100%	\$3.19
OGG	Install, integrate, network, and test (3) Medium Speed EDS for Terminal Main	\$-	\$1.10	100%	\$1.10
PHX	Purchase, install, integrate, network and test (1) Medium Speed EDS for Terminal 4	\$1.08	\$0.45	100%	\$1.53
PNS	Purchase, install, integrate, network and test (1) Medium Speed EDS for Terminal Main	\$0.42	\$0.12	100%	\$0.54
RDU	Purchase of (2) Medium Speed EDS for Terminal C West	\$2.16	\$-	100%	\$2.16
RNO	Install, integrate, network and test (3) Reduced Size EDS for Terminal Main	\$-	\$0.90	100%	\$0.90
ROC	Purchase of (6) Reduced Size EDS for Terminal Main	\$2.53	\$-	100%	\$2.53

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix N. EBSP FY 2009 Summary Spend Plan (continued)

Airport	Scope of Work	Purchase	Deployment	TSA Cost Share*	Total TSA FY 2009 Project Cost
SAN	Purchase, install, integrate, network and test (1) Medium Speed EDS for Terminal 2 East	\$1.08	\$0.24	100%	\$1.32
SFO	Purchase, install, integrate, network and test (4) Medium Speed EDS for Terminal C	\$4.32	\$1.43	100%	\$5.75
SNA	Purchase, install, integrate, network and test (4) Medium Speed EDS for Terminal C	\$4.32	\$2.11	100%	\$6.43
LSE	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.42	\$0.08	100%	\$0.50
PIT	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.42	\$0.08	100%	\$0.50
SMX	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.42	\$0.08	100%	\$0.50
ITO	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.42	\$0.08	100%	\$0.50
GPI	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.42	\$0.08	100%	\$0.50
MKK	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.42	\$0.08	100%	\$0.50
HLN	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.42	\$0.08	100%	\$0.50

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix N. EBSP FY 2009 Summary Spend Plan (continued)

Airport	Scope of Work	Purchase	Deployment	TSA Cost Share*	Total TSA FY 2009 Project Cost
CHA	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.42	\$0.08	100%	\$0.50
CHS	Purchase, install and test (3) Reduced Size EDS for Terminal Main	\$1.26	\$0.26	100%	\$1.52
CMI	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.42	\$0.08	100%	\$0.50
SUN	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.42	\$0.08	100%	\$0.50
GUC	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.42	\$0.08	100%	\$0.50
SAN-RS	Purchase, install, integrate, network and test (5) Reduced Size EDS for Terminal I	\$2.10	\$0.60	100%	\$2.70
PHL-RS	Purchase, install, integrate, network and test (3) Reduced Size EDS for Terminal B/C	\$1.26	\$0.89	100%	\$2.16
HDN	Install, integrate, network, and test (3) Reduced Size EDS for Terminal Main	\$-	\$1.24	100%	\$1.24
EGE	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.84	\$0.72	100%	\$1.56
ASE**	Purchase, install, integrate, network and test (2) Reduced Size EDS for Terminal Main				
SBA**	Purchase, install, integrate, network and test (2) Reduced Size EDS for Terminal Main	\$0.84	\$0.72	100%	\$1.56

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix N. EBSP FY 2009 Summary Spend Plan (continued)

Airport	Scope of Work	Purchase	Deployment	TSA Cost Share*	Total TSA FY 2009 Project Cost
TUS	Purchase, install, integrate, network and test (2) Reduced Size EDS for Terminal Main	\$1.68	\$0.33	100%	\$2.02
UTA	Purchase, install, integrate, network and test (2) Reduced Size EDS for Terminal Main	\$0.42	\$0.08	100%	\$0.5
RDM	Purchase, install, integrate, network and test (2) Reduced Size EDS for Terminal Main	\$0.84	\$0.72	100%	\$1.56
Recapitalization		\$20.75	\$5.0	100%	\$25.75
Total Purchase and Install		\$107.7	\$38.8		\$146.6

* TSA funds 100 percent of the Purchase and Install costs associated with each project

** ASE was canceled and replaced with SBA

Technology/Engineering Initiatives

Project Description	Total TSA FY 2009 Project Cost
Contracting Officer's Technical Representative/Engineering Initiatives	\$17.6
Security Technology Integrated Program	\$8.0
Advanced Surveillance Program	\$5.0
Operations Integration	\$2.0
Total	\$32.6

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix O. EBSP ARRA Summary Spend Plan

Summary

Section	Total	Revised Total*
Program Operations and Management	\$32.0	\$54.85
OTA – New Facility Modification Agreement Projects	\$598.1	\$499.2
EDS Purchase and Install	\$64.2	\$94.2
Technology/Engineering Initiatives	\$5.7	\$40.6
Total	\$700.0	\$688.85

*Revised Total: \$11 million shifted from EDS to PSP for ASP/CCTV projects

Program Operations and Management

Project Description	Total TSA FY 2009 ARRA Project Cost	Revised TSA FY 2009 ARRA Project Cost
Operations and Compliance/Interim Solutions		
- Moves, Adds and Changes	\$8.0	\$7.85
Program Support		
- Program, Resource and Data Management Services	\$6.8	\$10.0
- Testing Services	\$3.0	\$5.3
Engineering Support		
- Integration and Installation Management	\$7.8	\$24.8
- Engineering Technical and Design Support	\$2.6	\$3.1
Personnel Compensation and Benefits	\$3.8	\$3.8
Total	\$32.0	\$54.85

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix O. EBSP ARRA Summary Spend Plan (continued)

OTA – New Facility Modification Agreement Projects

Airport	Scope of Work	TSA Cost Share	Original TSA	Revised TSA
			FY 2009 ARRA Project Cost	FY 2009 ARRA Project Cost
HNL	OTA funding for the airport to construct a Checked Baggage Inspection System (CBIS) for Terminals 4, 5, 6, 7, 8	90%	\$43.50	\$24.50
OGG	OTA funding for the airport to construct a CBIS for Main Terminal	90%	\$18.50	\$7.20
PHL	OTA funding for the airport to construct a CBIS for Terminal A East	90%	\$53.00	\$26.60
SJC	OTA funding for the airport to construct a CBIS for Terminal B	90%	\$31.00	\$23.94
TLH	OTA funding for the airport to construct a CBIS for Main Terminal (canceled)	95%	\$15.00	-
PWM	OTA funding for the airport to construct a CBIS for Main Terminal	95%	\$13.30	\$13.50
SFO	OTA funding for the airport to construct a CBIS for Terminal 2	90%	\$30.00	\$15.35
SMF	OTA funding for the airport to construct a CBIS for Terminal B	90%	\$53.00	\$11.34

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix O. EBSP ARRA Summary Spend Plan (continued)

Airport	Scope of Work	TSA Cost Share	Original TSA FY 2009 ARRA Project Cost	Revised TSA FY 2009 ARRA Project Cost
JAC	OTA funding for the airport to construct a CBIS for Main Terminal	95%	\$8.80	\$6.21
HSV	OTA funding for the airport to construct a CBIS for Main Terminal	95%	\$27.50	\$1.50
MCO	OTA funding for the airport to construct a CBIS for East Terminal	90%	\$104.50	\$14.93
MCO	OTA funding for the airport to construct a CBIS for Disney Terminal		-	\$13.80
SNA	OTA funding for the airport to construct a CBIS for Terminals A and B (funded via FY09)	90%	\$51.30	
DAY	OTA funding for the airport to construct a CBIS for Main Terminal	95%	\$20.00	\$9.70
ATL	OTA funding for the airport to construct a CBIS for Main Terminal	90%	\$54.20	\$21.20
MSY	OTA funding for the airport to construct a CBIS for Main Terminal	90%	\$14.50	\$24.97

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix O. EBSP ARRA Summary Spend Plan (continued)

Airport	Scope of Work	TSA Cost Share	Original TSA FY 2009 ARRA Project Cost	Revised TSA FY 2009 ARRA Project Cost
CMH	OTA funding for the airport to construct a CBIS for Main Terminal	90%	\$60.00	\$26.50
STL	OTA funding for the airport to construct a CBIS for Main Terminal	90%	\$0.00	\$31.50
IAD	OTA funding for the airport to construct a CBIS for Main Terminal	90%	\$0.00	\$148.91
COD	OTA funding for the airport to construct a CBIS for Main Terminal	95%	\$0.00	\$0.35
HOU	OTA funding for the airport to construct a CBIS for Main Terminal	90%	\$0.00	\$0.51
PIE	OTA funding for the airport to construct a CBIS for Main Terminal	95%	\$0.00	\$0.63
BZN	OTA funding for the airport to construct a CBIS for Main Terminal	95%	\$0.00	\$6.80
TUL	OTA funding for the airport to construct a CBIS for Main Terminal	95%	\$0.00	\$4.72

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix O. EBSP ARRA Summary Spend Plan (continued)

Airport	Scope of Work	TSA Cost Share	Original TSA FY 2009 ARRA Project Cost	Revised TSA FY 2009 ARRA Project Cost
CLT	OTA funding for the airport to construct a CBIS for Main Terminal	90%	\$0.00	\$33.78
COS	OTA funding for the airport to construct a CBIS for Main Terminal	95%	\$0.00	\$7.41
LIT	OTA funding for the airport to construct a CBIS for Main Terminal	95%	\$0.0	\$8.96
SAT	OTA funding for the airport to construct a CBIS for Terminal 1/B	90%	\$0	\$14.39
Total			\$598.10	\$499.20

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix O. EBSP ARRA Summary Spend Plan (continued)

OTA – New Facility Modification Agreement Projects Reason for Change to Project Costs

Airport	Reason for Change
HNL	Cost validation
OGG	Cost to complete and cost validation
PHL	Cost validation
SJC	Cost validation
TLH	Airport Canceled Project
PWM	Cost validation
SFO	Cost validation
SMF	Cost validation after de-scoping of project
JAC	Cost validation
HSV	Cost validation
MCO	Cost validation
MCO	Of the \$104.5 million, Phase II has an Original Cost Estimate of \$13.2 million
SNA	Cost validation
DAY	Cost validation

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix O. EBSP ARRA Summary Spend Plan (continued)

Airport	Reason for Change
ATL	Cost validation
MSY	Cost validation
CMH	Cost validation
STL	New project
IAD	New project
COD	New project
HOU	New project
PIE	New project
BZN	New project
TUL	New project
CLT	New project
COS	New project
LIT	New project

Original projected costs were based solely on submitted airport applications. Validated projects found airports submitted applications with non-allowable/allocable construction-related costs, design fees and/or construction management.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix O. EBSP ARRA Summary Spend Plan (continued)

Reduced Size EDS

Scope of Work	TSA Cost Share	Total TSA FY 2009 ARRA Project Cost	Revised TSA FY 2009 ARRA Project Cost
Recapitalization	100%	\$43.2	\$58.2
ETD Only Airport	100%	\$21.0	\$36.0
Total		\$64.2	\$94.2

Technology/Engineering Initiatives

Project Description	Total TSA FY 2009 ARRA Project Cost	Revised TSA FY 2009 ARRA Project Cost
Engineering Initiatives	\$3.5	\$0
Advanced Surveillance Program	\$2.2	\$40.6
- <i>Boise Air Terminal/Gowen Field (BOI)</i>	\$0.3	\$0.3
- <i>Ronald Reagan Washington National (DCA)</i>	\$1.1	\$1.1
- <i>Cincinnati/Northern Kentucky International (CVG)</i>	\$.2	\$.2
- <i>Spokane International (GEG)</i>	\$0.4	\$0.4
- <i>Gerald R. Ford International (GRR)</i>	\$.2	\$.2
- <i>Washington Dulles International (IAD)</i>	\$0	\$5.8
- <i>Will Rogers World (OKC)</i>	\$0	\$4.2
- <i>Chicago Midway International Airport (MDW)</i>	\$0	\$6.8
- <i>Eppley Airfield (OMA)</i>	\$0	\$4.0

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix O. EBSP ARRA Summary Spend Plan (continued)

Project Description	Total TSA FY 2009 ARRA Project Cost	Revised TSA FY 2009 ARRA Project Cost
- <i>James M Cox Dayton International Airport (DAY)</i>	\$0	\$3.0
- <i>Kansas City International (MCI)</i>	\$0	\$5.8
- <i>Adams Field (LIT)</i>	\$0	\$3.0
- <i>Tampa International (TPA)</i>	\$0	\$6.0
Total	\$5.7	\$40.6

Numbers may not add due to rounding.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix P. EBSP FY 2009 Obligation Data

Obligation Schedule

Obligation dates and selected airports are subject to change based on airport schedules and contract negotiations.

Airport	Scope of Work	Project Cost \$ in Millions	Planned Obligation Date
Program Operations and Management			
N/A	Ops Compliance, Program Support, Engineering Support, TSIF Support and P, C and B	\$97.5	Ongoing through Sept-09
LOI Projects			
JFK	LOI Funding for the airport to construct a CBIS for Terminals 2, 3, 4 and 7	\$78.0	May-09
EWR	LOI funding for the airport to construct a CBIS for Terminals A, B and C	\$60.0	May-09
LGA	LOI funding for the airport to construct a CBIS for Terminals USAir and CTB	\$62.0	May-09
EDS Install and Purchase Projects			
EWR	Purchase, install, integrate, network and test (3) Medium Speed EDS	\$4.48	P-Jun-09 I-Oct-09
ORD	Purchase, install, integrate, network and test (4) Medium Speed EDS for Terminal 1B-South	\$5.87	P-Jun-09 I-Dec-09

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix P. EBSP FY 2009 Obligation Data (continued)

Airport	Scope of Work	Project Cost \$ in Millions	Planned Obligation Date
EDS Install and Purchase Projects (continued)			
CVG	Purchase, install, integrate, network and test (5) Medium Speed EDS for Terminal 3	\$7.56	P-Jun-09 I-Aug-09
MCO	Purchase, install, integrate, network and test (7) Medium Speed EDS for Terminal Central East	\$10.21	P-Jun-09 I-Aug-09
MIA	Purchase, install, integrate, network and test (8) Medium Speed EDS for Terminal East/Cruise Matrix	\$11.27	P-Jun-09 I-Sep-09
IAH	Purchase, install, integrate, network and test (4) Medium Speed EDS for Terminal D	\$5.87	P-Jun-09 I-Dec-09
ACK	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.54	P-Jan-09 I-Feb-09
SAT	Purchase, install, integrate, network and test (7) Medium Speed EDS for Terminal 1/B	\$9.98	P-Jun-09 I-Oct-09
PFN	Purchase, install, integrate, network and test (2) Medium Speed EDS for Terminal New	\$3.08	P-Jun-09 I-Dec-09
SJC	Purchase, install, integrate, network and test (8) Medium Speed EDS for Terminal A/B	\$12.64	P-Jun-09 I-Jul-09 Dec-09
AMA	Purchase, install, integrate, network and test (2) Reduced Size EDS for Terminal Main	\$1.66	P-Mar-09 I-May-09
MFR	Purchase, install, integrate, network and test (2) Reduced Size EDS for Terminal Main	\$1.88	P-Jan-09 I-May-09

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix P. EBSP FY09 Obligation Data (continued)

Airport	Scope of Work	Project Cost \$ in Millions	Planned Obligation Date
EDS Install and Purchase Projects (continued)			
TLH	Purchase, install, integrate, network and test (2) Medium Speed EDS for Terminal Main	\$3.19	P-Jun-09 I-Nov-09
OGG	Install, integrate, network and test (3) Medium Speed EDS for Terminal Main	\$1.10	P-warehouse* I-Aug-09
PHX	Purchase, install, integrate, network and test (1) Medium Speed EDS for Terminal 4	\$1.53	P-Jan-09 I-Aug-09
PNS	Purchase, install, integrate, network and test (1) Medium Speed EDS for Terminal Main	\$0.54	P-Jan-09 I-Jul-09
RDU	Purchase of (2) Medium Speed EDS for Terminal C West	\$2.16	P-Sep-09 I-Mar-10
RNO	Install, integrate, network and test (3) Reduced Size EDS for Terminal Main	\$0.90	P-relocation* I-Aug-09
ROC	Purchase of (6) Reduced Size EDS for Terminal Main	\$2.53	P-Mar-09 I-May-09 *
SAN	Purchase, install, integrate, network and test (1) Medium Speed EDS for Terminal 2 East	\$1.32	P-Jan-09 I-Aug-09
SFO	Purchase, install, integrate, network and test (4) Medium Speed EDS for Terminal 2	\$5.75	P-Jun-09 I-Jan-10

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix P. EBSP FY 2009 Obligation Data (continued)

Airport	Scope of Work	Project Cost \$ in Millions	Planned Obligation Date
EDS Install and Purchase Projects (continued)			
SNA	Purchase, install, integrate, network and test (4) Medium Speed EDS for Terminal C	\$6.43	P-Jun-09 I-Nov-09
LSE	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.50	P-Mar-09 I-May-09
PIT	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.50	P-Mar-09 I-Aug-09
SMX	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.50	P-Mar-09 I-Jun-09
ITO	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.50	P-Mar-09 I-Jun-09
GPI	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.50	P-Mar-09 I-Jun-09
MKK	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.50	P-Mar-09 I-Jun-09
HLN	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.50	P-Mar-09 I-Jun-09
CHA	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.50	P-Jan-09 I-Mar-09
CHS	Purchase, install and test (3) Reduced Size EDS for Terminal Main	\$1.52	P-Jan-09 I-Feb-09

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix P. EBSP FY 2009 Obligation Data (continued)

Airport	Scope of Work	Project Cost \$ in Millions	Planned Obligation Date
EDS Install and Purchase Projects (continued)			
CMI	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.50	P-Jan-09 I-Apr-09
SUN	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.50	P-Jan-09 I-Apr-09
GUC	Purchase, install and test (1) Reduced Size EDS for Terminal Main	\$0.50	P-Mar-09 I-May-09
SAN-RS	Purchase, install, integrate, network and test (5) Reduced Size EDS for Terminal 1	\$2.70	P-Jan-09 I-Apr-09
PHL-RS	Purchase, install, integrate, network, and test (3) Reduced Size EDS for Terminal B/C	\$2.16	P-Mar-09 I-May-09
HDN	Install, integrate, network and test (3) Reduced Size EDS for Terminal Main	\$1.24	P-Mar-09 I-May-09
EGE	Purchase, install, integrate, network and test (2) Reduced Size EDS for Terminal Main	\$1.56	P-Mar-09 I-Jun-09
ASE	Purchase, install, integrate, network and test (2) Reduced Size EDS for Terminal Main		Project canceled and replaced with SBA
SBA	Purchase, install, integrate, network and test (2) Reduced Size EDS for Terminal Main	\$1.56	P-Mar-09 I-Jul-09

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix P. EBSP FY 2009 Obligation Data (continued)

Airport	Scope of Work	Project Cost \$ in Millions	Planned Obligation Date
EDS Install and Purchase Projects (continued)			
TUS	Purchase, install, integrate, network and test (4) Reduced Size EDS for Terminal Main	\$2.02	P-Jan-09 I-Mar-09
UTA	Purchase, install, integrate, network and test (1) Reduced Size EDS for Terminal Main	\$0.50	P-Mar-09 I-Jun-09
RDM	Purchase, install, integrate, network and test (3) Reduced Size EDS for Terminal Main	\$1.56	P-Jan-09 I-Feb-09

P = purchase

I = install

DEVIATION FROM ORIGINAL SPEND PLAN

After further evaluation, it was determined the current configuration at the Aspen-Pitkin County/Sardy Field (ASE) airport was sufficient to support the needs of the airport. The passenger throughput did not increase as anticipated. The Santa Barbara Municipal (SBA) airport was identified as an airport with increased throughput and served as a replacement airport for the ASE project. The equipment purchase and installation at SBA was comparable to ASE and there were no significant funding changes. The project timeline and schedule were also closely aligned and caused no changes to the current spend plan.

Airport	Technology Purchases	Project Cost \$ in Millions	Planned Obligation Date
N/A	Medium Throughput GE—March through September L3—September	\$84.74	Mar-09 through Sept-09
N/A	Reduced Size Reveal—January through September L3—September	\$23.00	Jan-09 through Sept-09

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix P. EBSP FY 2009 Obligation Data (continued)

Airport	Scope of Work	Project Cost \$ in millions	Planned Obligation Date
New Facility Modification Agreement Projects			
ORD	OTA funding for the airport to construct a CBIS for Terminal 1-B South	\$19.8	May-09
ICT	OTA funding for the airport to construct a CBIS for Terminal Main	\$8.25	Sep-09
SAT	OTA funding for the airport to construct a CBIS for Terminal 1/B (Funded via ARRA)		
FAT	OTA funding for the airport to construct a CBIS for Terminal Main	\$3.75	Jun-09
MSP	OTA funding for the airport to construct a CBIS for the Lindbergh Terminal	\$8.0	Sep-09
TRI	OTA funding for the airport to construct a CBIS for Terminal Main	\$3.25	Sep-09
AMA	OTA funding for the airport to construct a CBIS for Terminal Main	\$8.25	Sep-09
PFN	OTA funding for the airport to construct a CBIS for New Terminal	\$7.25	Jul-09
SNA	OTA funding for the airport to construct a CBIS for Terminals A and B	\$8.77	Sep-09

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix P. EBSP FY 2009 Obligation Data (continued)

Airport	Scope of Work	Project Cost in millions	Planned Obligation Date
Technology/Engineering Initiatives			
N/A	COTR Initiatives, STIP, ASP, OI and Engineering Initiatives	\$32.6	Ongoing through Sept-09

- Funding provided in FY 2008

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix Q. EBSP ARRA Obligation Data

Obligation Schedule

Airport Other Transactional Agreements	Facility Modification	Planned Month for Obligation
HNL	\$24.50	Aug-09
OGG	\$7.20	Aug-09
PHL	\$26.60	Jun-09
SJC	\$23.94	Sep-09
TLH	-	-
PWM	\$13.50	Aug-09
SFO	\$15.35	Jun-09
SMF	\$11.34	Aug-09
JAC	\$6.21	Jun-09
HSV	\$1.50	Sep-09
MCO (East)	\$14.93	July-09
MCO (Disney)	\$13.80	Sep-09
SNA		
DAY	\$9.70	Aug-09
ATL	\$21.20	Sep-09
MSY	\$24.97	Sept 09, Mar-09
CMH	\$26.50	Sep-09
STL	\$31.50	Sep-09
IAD	\$148.91	Sep-09
COD	\$0.35	Sep-09
HOU	\$0.51	Sep-09
PIE	\$0.63	Oct-09
BZN	\$6.80	Dec-09
TUL	\$4.72	Dec-09
CLT	\$33.78	Jan-10
COS	\$7.41	Jan-10
LIT	\$8.96	Nov-09
SAT	\$14.39	Sep-09
Total	\$499.2 millions	

Obligation dates and selected airports are subject to change based on airport schedules and contract negotiations.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix R. EBSP FY 2009 Milestones

Project Timelines – New Facility Modification Agreement Projects

Project Timelines – LOI Projects

Major Milestones	Estimated Completion Date
La Guardia (LGA)	
Initiate second year of LOI evaluation	Dec-08
Airports submit updated cost information to the Transportation Security Administration (TSA)	Apr-09
Modify existing LOI for additional funding requirements*	Jul-09
Newark Liberty International (EWR)	
Initiate second year of LOI evaluation	Dec-08
Airports submit updated cost information to TSA	Apr-09
Modify existing LOI for additional funding requirements*	Jul-09
John F. Kennedy International (JFK)	
Initiate second year of LOI evaluation	Dec-08
Airports submit updated cost information to TSA	Apr-09
Modify existing LOI for additional funding requirements*	Jul-09

*LOIs require congressional notification 3 days before contract execution.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix R. EBSP FY 2009 Milestones (continued)

Project Timelines – EDS Purchase and Install Projects

Major Milestones	Estimated Completion Date
Newark Liberty International (EWR)	
EDS Deliver	Oct-09
Installation and Integration	Oct-09
Independent Verification and Validation (IV&V)/Commissioning	Mar-10
Live Bag Screening	Apr-10
Decommissioning	May-10
Chicago O'Hare International (ORD)	
EDS Delivery	Dec-09
Installation and Integration	Dec-09
IV&V/Commissioning	Apr-10
Live Bag Screening	May-10
Decommissioning	Jun-10
Cincinnati/Northern Kentucky International (CVG)	
EDS Delivery	Feb-09
Installation and Integration	Aug-09
IV&V/Commissioning	Jan-10
Live Bag Screening	Feb-10
Decommissioning	Mar-10
Orlando International (MCO)	
EDS Delivery	Feb-09
Installation and Integration	Aug-09
IV&V/Commissioning	Jan-10
Live Bag Screening	Feb-10
Decommissioning	Mar-10
Miami International (MIA)	
EDS Delivery	Mar-09
Installation and Integration	Sep-09
IV&V/Commissioning	Feb-10
Live Bag Screening	Mar-10
Decommissioning	Apr-10

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix R. EBSP FY 2009 Milestones (continued)

Project Timelines – EDS Purchase and Install Projects (continued)

Major Milestones	Estimated Completion Date
George Bush Intercontinental/Houston (IAH)	
EDS Delivery	Dec-09
Installation and Integration	Dec-09
IV&V/Commissioning	Mar-10
Live Bag Screening	Apr-10
Decommissioning	May-10
Nantucket Memorial (ACK)	
EDS Delivery	Feb-09
Installation and Integration	Feb-09
Decommissioning	N/A
San Antonio International (SAT)	
EDS Delivery	Oct-09
Installation and Integration	Oct-09
IV&V/Commissioning	Jun-10
Live Bag Screening	Jul-10
Decommissioning	Aug-10
Panama City-Bay County International (PFN)	
EDS Delivery	Dec-09
Installation and Integration	Dec-09
IV&V/Commissioning	Apr-10
Live Bag Screening	May-10
Decommissioning	Jun-10
Norman Y. Mineta San Jose International (SJC)	
EDS Delivery	Jul-09 and Dec-09
Installation and Integration	Jul-09 and Jan-10
IV&V/Commissioning	Jan-10 and Jul-10
Live Bag Screening	Feb-10 and Aug-10
Decommissioning	Mar-10 and Sep-10
Rick Husband Amarillo International (AMA)	
EDS Delivery	May-09
Installation and Integration	May-09
Decommissioning	N/A

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix R. EBSP FY 2009 Milestones (continued)

Project Timelines – EDS Purchase and Install Projects (continued)

Major Milestones	Estimated Completion Date
Rogue Valley International-Medford (MFR)	
EDS Delivery	Feb-09
Installation and Integration	Aug-09
Decommissioning	N/A
Tallahassee Regional (TLH)	
EDS Delivery	Oct-09
Installation and Integration	Nov-09
IV&V/Commissioning	Apr-10
Live Bag Screening	May-10
Decommissioning	Jun-10
Kahului (OGG)	
EDS Delivery	Feb-09
Installation and Integration	Aug-09
IV&V/Commissioning	Jan-10
Live Bag Screening	Feb-10
Decommissioning	Mar-10
Phoenix Sky Harbor International Airport (PHX)	
EDS Delivery	Feb-09
Installation and Integration	Aug-09
IV&V/Commissioning	Jan-10
Live Bag Screening	Feb-10
Decommissioning	Mar-10
Pensacola Regional (PNS)	
EDS Delivery	Jan-09
Installation and Integration	Jul-09
Decommissioning	Mar-10
Raleigh-Durham International (RDU)	
EDS Delivery	Oct-09
Installation and Integration	Mar-10
IV&V/Commissioning	Aug-10
Live Bag Screening	Sep-10
Decommissioning	Oct-10

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix R. EBSP FY 2009 Milestones (continued)

Project Timelines – EDS Purchase and Install Projects (continued)

Major Milestones	Estimated Completion Date
Reno/Tahoe International (RNO)	
EDS Delivery	Jul-09
Installation and Integration	Aug-09
Decommissioning	N/A
Greater Rochester International (ROC)	
EDS Delivery	May-09
Installation and Integration	May-09
Decommissioning	N/A
San Diego International (SAN)	
EDS Delivery	Feb-09
Installation and Integration	Aug-09
IV&V/Commissioning	Jan-10
Live Bag Screening	Feb-10
Decommissioning	Mar-10
San Francisco International (SFO)	
EDS Delivery	Dec-09
Installation and Integration	Jan-10
IV&V/Commissioning	Feb-10
Live Bag Screening	Mar-10
Decommissioning	Apr-10
John Wayne Airport-Orange County (SNA)	
EDS Delivery	Nov-09
Installation and Integration	Nov-09
IV&V/Commissioning	Apr-10
Live Bag Screening	May-10
Decommissioning	Jun-10
La Crosse Municipal (LSE)	
EDS Delivery	May-09
Installation and Integration	May-09
Decommissioning	N/A
Pittsburgh International (PIT)	
EDS Delivery	Aug-09
Installation and Integration	Aug-09
Decommissioning	N/A

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix R. EBSP FY 2009 Milestones (continued)

Project Timelines – EDS Purchase and Install Projects (continued)

Major Milestones	Estimated Completion Date
Santa Maria Public Airport (SMX)	
EDS Delivery	Jun-09
Installation and Integration	Jun-09
Decommissioning	N/A
Hilo International (ITO)	
EDS Delivery	Jun-09
Installation and Integration	Jun-09
Decommissioning	N/A
Glacier Park International (GPI)	
EDS Delivery	Jun-09
Installation and Integration	Jun-09
Decommissioning	N/A
Molokai Airport (MKK)	
EDS Delivery	Jun-09
Installation and Integration	Jun-09
Decommissioning	N/A
Helena Regional (HLN)	
EDS Delivery	Jun-09
Installation and Integration	Jun-09
Decommissioning	N/A
Lovell Field (CHA)	
EDS Delivery	Mar-09
Installation and Integration	Mar-09
Decommissioning	N/A
Charleston AFB/International (CHS)	
EDS Delivery	Feb-09
Installation and Integration	Feb-09
Decommissioning	N/A
University of Illinois-Willard (CMI)	
EDS Delivery	Apr-09
Installation and Integration	Apr-09
Decommissioning	N/A

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix R. EBSP FY 2009 Milestones (continued)

Project Timelines – EDS Purchase and Install Projects (continued)

Major Milestones	Estimated Completion Date
Friedman Memorial (SUN)	
EDS Delivery	Apr-09
Installation and Integration	Apr-09
Decommissioning	N/A
Gunnison-Crested Butte Regional (GUC)	
EDS Delivery	May-09
Installation and Integration	May-09
Decommissioning	N/A
San Diego International (SAN-RS)	
EDS Delivery	Apr-09
Installation and Integration	Apr-09
Decommissioning	N/A
Philadelphia International (PHL)	
EDS Delivery	May-09
Installation and Integration	May-09
Decommissioning	N/A
Yampa Valley (HDN)	
EDS Delivery	May-09
Installation and Integration	May-09
Decommissioning	N/A
EDS Delivery	Jun-09
Eagle County Regional (EGE)	
EDS Delivery	Jun-09
Installation and Integration	Jun-09
Decommissioning	N/A
Aspen-Pitkin County/Sardy Field (ASE)	
EDS Delivery	Project canceled
Installation and Integration	Replaced with SBA
Decommissioning	
Santa Barbara Municipal (SBA)	
EDS Delivery	Jun-09
Installation and Integration	Jul-09
Decommissioning	N/A

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix R. EBSP FY 2009 Milestones (continued)

Project Timelines – EDS Purchase and Install Projects (continued)

Major Milestones	Estimated Completion Date
Tucson International (TUS)	
EDS Delivery	Mar-09
Installation and Integration	Mar-09
Decommissioning	N/A
Tunica Municipal (UTA)	
EDS Delivery	Jun-09
Installation and Integration	Jun-09
Decommissioning	N/A
Roberts Field (RDM)	
EDS Delivery	Feb-09
Installation and Integration	Feb-09
Decommissioning	N/A

Standalone EDS equipment is tested at time of delivery. The EDS equipment is usually operational 1 week after installation and testing. Standalone equipment only requires a decommissioning when a replacement is delivered. When additional units are delivered, no decommissioning is necessary.

An airport's construction schedule generally affects the delivery of the TSA equipment and is out of TSA's control. When an airport construction schedule slips, delivery timelines are adjusted accordingly.

Airport accepts delivery of equipment, depending on construction schedule. The equipment is typically not operational for another 3-6 months for inline systems and 1 week for standalone EDS equipment after installation, depending on airport's schedule. TSA awards a delivery order to the Original Equipment Manufacturer for services.

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix R. EBSP FY 2009 Milestones (continued)

Project Timelines – New Facility Modification Agreement Projects

Major Milestones	Estimated Completion Date
Chicago O'Hare International (ORD)	
Notification letter sent to airport	February 10, 2009
Draft other transaction agreement (OTA) sent to airport to review the terms and conditions	March 22, 2009
Airports submit updated cost information to TSA	February 19, 2009
Cost validations updated based on information provided by the airport	April 3, 2009
Negotiation meetings scheduled with the airport	April 28, 2009
Negotiations completed and OTA executed	May 2009
Wichita Mid-Continent (ICT)	
Notification letter sent to airport	February 10, 2009
Draft OTA sent to airport to review the terms and conditions	March 22, 2009
Airports submit updated cost information to TSA	February 27, 2009
Cost validations updated based on information provided by the airport	late April 2009
Negotiation meetings scheduled with the airport	June 2009
Negotiations completed and OTA executed	September 2009
Fresno Yosemite International (FAT)	
Notification letter sent to airport	February 23, 2009
Draft OTA sent to airport to review the terms and conditions	February 9, 2009
Airports submit updated cost information to TSA	February 11, 2009
Cost validations updated based on information provided by the airport	March 31, 2009
Negotiation meetings scheduled with the airport	May 2009
Negotiations completed and OTA executed	June 2009

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix R. EBSP FY 2009 Milestones (continued)

Project Timelines – New Facility Modification Agreement Projects (continued)

Major Milestones	Estimated Completion Date
Minneapolis-St. Paul International/Wold-Chamberlain (MSP)	
Notification letter sent to airport	February 10, 2009
Draft OTA sent to airport to review the terms and conditions	March 22, 2009
Airports submit updated cost information to TSA	April 1, 2009
Cost validations updated based on information provided by the airport	April 3, 2009
Negotiation meetings scheduled with the airport	June 2009
Negotiations completed and OTA executed	September 2009
Tri-Cities Regional TN/VA (TRI)	
Notification letter sent to airport	February 10, 2009
Draft OTA sent to airport to review the terms and conditions	March 13, 2009
Airports submit updated cost information to TSA	late March 2009
Cost validations updated based on information provided by the airport	April 9, 2009
Negotiation meetings scheduled with the airport	April 28, 2009
Negotiations completed and OTA executed	September 2009
Rick Husband Amarillo International (AMA)	
Notification letter sent to airport	February 10, 2009
Draft OTA sent to airport to review the terms and conditions	April 6, 2009
Airports submit updated cost information to TSA	February 24, 2009
Cost validations updated based on information provided by the airport	March 25, 2009
Negotiation meetings scheduled with the airport	April 28, 2009
Negotiations completed and OTA executed	September 2009

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix R. EBSP FY 2009 Milestones (continued)

Project Timelines – New Facility Modification Agreement Projects (continued)

Major Milestones	Estimated Completion Date
Panama City-Bay County International (PFN)	
Notification letter sent to airport	February 9, 2009
Draft OTA sent to airport to review the terms and conditions	February 9, 2009
Airports submit updated cost information to TSA	March 20, 2009
Cost validations updated based on information provided by the airport	April 9, 2009
Negotiation meetings scheduled with the airport	June 2009
Negotiations completed and OTA executed	July 2009
John Wayne Airport-Orange County (SNA)	
Notification letter sent to airport	March 2009
Draft OTA sent to airport to review the terms and conditions	mid March 2009
Airports submit updated cost information to TSA	early April 2009
Cost validations updated based on information provided by the airport	mid April 2009
Negotiation meetings scheduled with the airport	early September 2009
Negotiations completed and OTA executed	Late September 2009

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix S. EBSP ARRA Milestones

Project Timelines – New Facility Modification Agreement Projects

Major Milestones	Estimated Completion Date
Honolulu International Airport (HNL)	
Notification letter sent to airport	March 2009
Draft other transaction agreement (OTA) sent to airport to review the terms and conditions	mid March 2009
Airports submit updated cost information to Transportation Security Administration (TSA)	late March 2009
Cost validations updated based on information provided by the airport	mid April 2009
Negotiation meetings scheduled with the airport	early June 2009
Negotiations completed and OTA executed	August 2009
Kahului Airport (OGG)	
Notification letter sent to airport	March 2009
Draft OTA sent to airport to review the terms and conditions	early March 2009
Airports submit updated cost information to TSA	early March 2009
Cost validations updated based on information provided by the airport	mid March 2009
Negotiation meetings scheduled with the airport	early June 2009
Negotiations completed and OTA executed	late August 2009
Philadelphia International Airport (PHL)	
Notification letter sent to airport	March 2009
Draft OTA sent to airport to review the terms and conditions	mid March 2009
Airports submit updated cost information to TSA	late March 2009
Cost validations updated based on information provided by the airport	mid April 2009
Negotiation meetings scheduled with the airport	early May 2009
Negotiations completed and OTA executed	mid June 2009

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix S. EBSP ARRA Milestones (continued)

Project Timelines – New Facility Modification Agreement Projects (continued)

Major Milestones	Estimated Completion Date
Normal Y. Mineta San Jose International Airport (SJC)	
Notification letter sent to airport	March 2009
Draft OTA sent to airport to review the terms and conditions	mid March 2009
Airports submit updated cost information to TSA	mid March 2009
Cost validations updated based on information provided by the airport	early May 2009
Negotiation meetings scheduled with the airport	late June 2009
Negotiations completed and OTA executed	late September 2009
Tallahassee Regional Airport (TLH)	
Notification letter sent to airport	March 2009
Draft OTA sent to airport to review the terms and conditions	mid March 2009
Airports submit updated cost information to TSA	early April 2009
Cost validations updated based on information provided by the airport	mid April 2009
Negotiation meetings scheduled with the airport	Project canceled by airport
Negotiations completed and OTA executed	N/A
Portland International Jetport (PWM)	
Notification letter sent to airport	March 2009
Draft OTA sent to airport to review the terms and conditions	mid March 2009
Airports submit updated cost information to TSA	mid March 2009
Cost validations updated based on information provided by the airport	early April 2009
Negotiation meetings scheduled with the airport	early June 2009
Negotiations completed and OTA executed	late August 2009

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix S. EBSP ARRA Milestones (continued)

Project Timelines – New Facility Modification Agreement Projects (continued)

Major Milestones	Estimated Completion Date
San Francisco International Airport (SFO)	
Notification letter sent to airport	March 2009
Draft OTA sent to airport to review the terms and conditions	mid March 2009
Airports submit updated cost information to TSA	late March 2009
Cost validations updated based on information provided by the airport	late March 2009
Negotiation meetings scheduled with the airport	late April 2009
Negotiations completed and OTA executed	early June 2009
Sacramento International Airport (SMF)	
Notification letter sent to airport	March 2009
Draft OTA sent to airport to review the terms and conditions	mid March 2009
Airports submit updated cost information to TSA	early April 2009
Cost validations updated based on information provided by the airport	mid April 2009
Negotiation meetings scheduled with the airport	late May 2009
Negotiations completed and OTA executed	August 2009
Jackson Hole Airport (JAC)	
Notification letter sent to airport	March 2009
Draft OTA sent to airport to review the terms and conditions	mid March 2009
Airports submit updated cost information to TSA	late March 2009
Cost validations updated based on information provided by the airport	mid April 2009
Negotiation meetings scheduled with the airport	late April 2009
Negotiations completed and OTA executed	mid June 2009

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix S. EBSA ARRA Milestones (continued)

Major Milestones	Estimated Completion Date
Huntsville International – Carl T. Jones Field Airport (HSV)	
Notification letter sent to airport	March 2009
Draft OTA sent to airport to review the terms and conditions	mid March 2009
Airports submit updated cost information to TSA	early April 2009
Cost validations updated based on information provided by the airport	mid April 2009
Negotiation meetings scheduled with the airport	early September 2009
Negotiations completed and OTA executed	late September 2009
Orlando International Airport (MCO) – East Terminal	
Notification letter sent to airport	March 2009
Draft OTA sent to airport to review the terms and conditions	mid March 2009
Airports submit updated cost information to TSA	early April 2009
Cost validations updated based on information provided by the airport	mid May 2009
Negotiation meetings scheduled with the airport	early June 2009
Negotiations completed and OTA executed	late July 2009
Orlando International Airport (MCO) – Disney Terminal	
Notification letter sent to airport	March 2009
Draft OTA sent to airport to review the terms and conditions	mid March 2009
Airports submit updated cost information to TSA	early April 2009
Cost validations updated based on information provided by the airport	mid April 2009
Negotiation meetings scheduled with the airport	early September 2009
Negotiations completed and OTA executed	late September 2009

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix S. EBSP ARRA Milestones (continued)

Project Timelines – New Facility Modification Agreement Projects (continued)

Major Milestones	Estimated Completion Date
James M. Cox Dayton International Airport (DAY)	
Notification letter sent to airport	March 2009
Draft OTA sent to airport to review the terms and conditions	mid March 2009
Airports submit updated cost information to TSA	late April 2009
Cost validations updated based on information provided by the airport	late April 2009
Negotiation meetings scheduled with the airport	late July 2009
Negotiations completed and OTA executed	late August 2009
Port Columbus International (CMH)	
Notification letter sent to airport	March 2009
Draft OTA sent to airport to review the terms and conditions	mid March 2009
Airports submit updated cost information to TSA	late March 2009
Cost validations updated based on information provided by the airport	early April 2009
Negotiation meetings scheduled with the airport	early July 2009
Negotiations completed and OTA executed	late September 2009
Hartsfield – Jackson Atlanta International Airport (ATL)	
Notification letter sent to airport	March 2009
Draft OTA sent to airport to review the terms and conditions	mid March 2009
Airports submit updated cost information to TSA	late March 2009
Cost validations updated based on information provided by the airport	early April 2009
Negotiation meetings scheduled with the airport	early July 2009
Negotiations completed and OTA executed	late September 2009

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix S. EBSP ARRA Milestones (continued)

Project Timelines – New Facility Modification Agreement Projects (continued)

Major Milestones	Estimated Completion Date
Louis Armstrong New Orleans International Airport (MSY)	
Notification letter sent to airport	March 2009
Draft OTA sent to airport to review the terms and conditions	mid March 2009
Airports submit updated cost information to TSA	early April 2009
Cost validations updated based on information provided by the airport	mid May 2009
Negotiation meetings scheduled with the airport	early October 2009
Negotiations completed and OTA executed	March 2009
Lambert-Saint Louis International Airport (STL)	
Notification letter sent to airport	July 2009
Draft OTA sent to airport to review the terms and conditions	July 2009
Airports submit updated cost information to TSA	late July 2009
Cost validations updated based on information provided by the airport	mid August 2009
Negotiation meetings scheduled with the airport	late August 2009
Negotiations completed and OTA executed	late September 2009
Washington Dulles International Airport (IAD)	
Notification letter sent to airport	July 2009
Draft OTA sent to airport to review the terms and conditions	July 2009
Airports submit updated cost information to TSA	late July 2009
Cost validations updated based on information provided by the airport	mid August 2009
Negotiation meetings scheduled with the airport	late August 2009
Negotiations completed and OTA executed	late September 2009

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix S. EBSP ARRA Milestones (continued)

Project Timelines – New Facility Modification Agreement Projects (continued)

Major Milestones	Estimated Completion Date
Yellowstone Regional Airport (COD)	
Notification letter sent to airport	July 2009
Draft OTA sent to airport to review the terms and conditions	July 2009
Airports submit updated cost information to TSA	late July 2009
Cost validations updated based on information provided by the airport	mid August 2009
Negotiation meetings scheduled with the airport	late August 2009
Negotiations completed and OTA executed	late September 2009
William P. Hobby Airport (HOU)	
Notification letter sent to airport	July 2009
Draft OTA sent to airport to review the terms and conditions	July 2009
Airports submit updated cost information to TSA	late July 2009
Cost validations updated based on information provided by the airport	mid August 2009
Negotiation meetings scheduled with the airport	late August 2009
Negotiations completed and OTA executed	late September 2009
St. Petersburg-Clearwater International Airport (PIE)	
Notification letter sent to airport	July 2009
Draft OTA sent to airport to review the terms and conditions	July 2009
Airports submit updated cost information to TSA	late July 2009
Cost validations updated based on information provided by the airport	mid August 2009
Negotiation meetings scheduled with the airport	early September 2009
Negotiations completed and OTA executed	late October 2009

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

Appendix S. EBSP ARRA Milestones (continued)

Project Timelines – New Facility Modification Agreement Projects (continued)

Major Milestones	Estimated Completion Date
Gallatin Field Airport (BZN)	
Notification letter sent to airport	July 2009
Draft OTA sent to airport to review the terms and conditions	July 2009
Airports submit updated cost information to TSA	late July 2009
Cost validations updated based on information provided by the airport	mid August 2009
Negotiation meetings scheduled with the airport	early September 2009
Negotiations completed and OTA executed	late December 2009
Tulsa International Airport (TUL)	
Notification letter sent to airport	July 2009
Draft OTA sent to airport to review the terms and conditions	July 2009
Airports submit updated cost information to TSA	late July 2009
Cost validations updated based on information provided by the airport	mid August 2009
Negotiation meetings scheduled with the airport	late September 2009
Negotiations completed and OTA executed	late December 2009
Charlotte/Douglas International Airport (CLT)	
Notification letter sent to airport	July 2009
Draft OTA sent to airport to review the terms and conditions	July 2009
Airports submit updated cost information to TSA	late July 2009
Cost validations updated based on information provided by the airport	mid August 2009
Negotiation meetings scheduled with the airport	mid October 2009
Negotiations completed and OTA executed	January 2010

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

FOR OFFICIAL USE ONLY

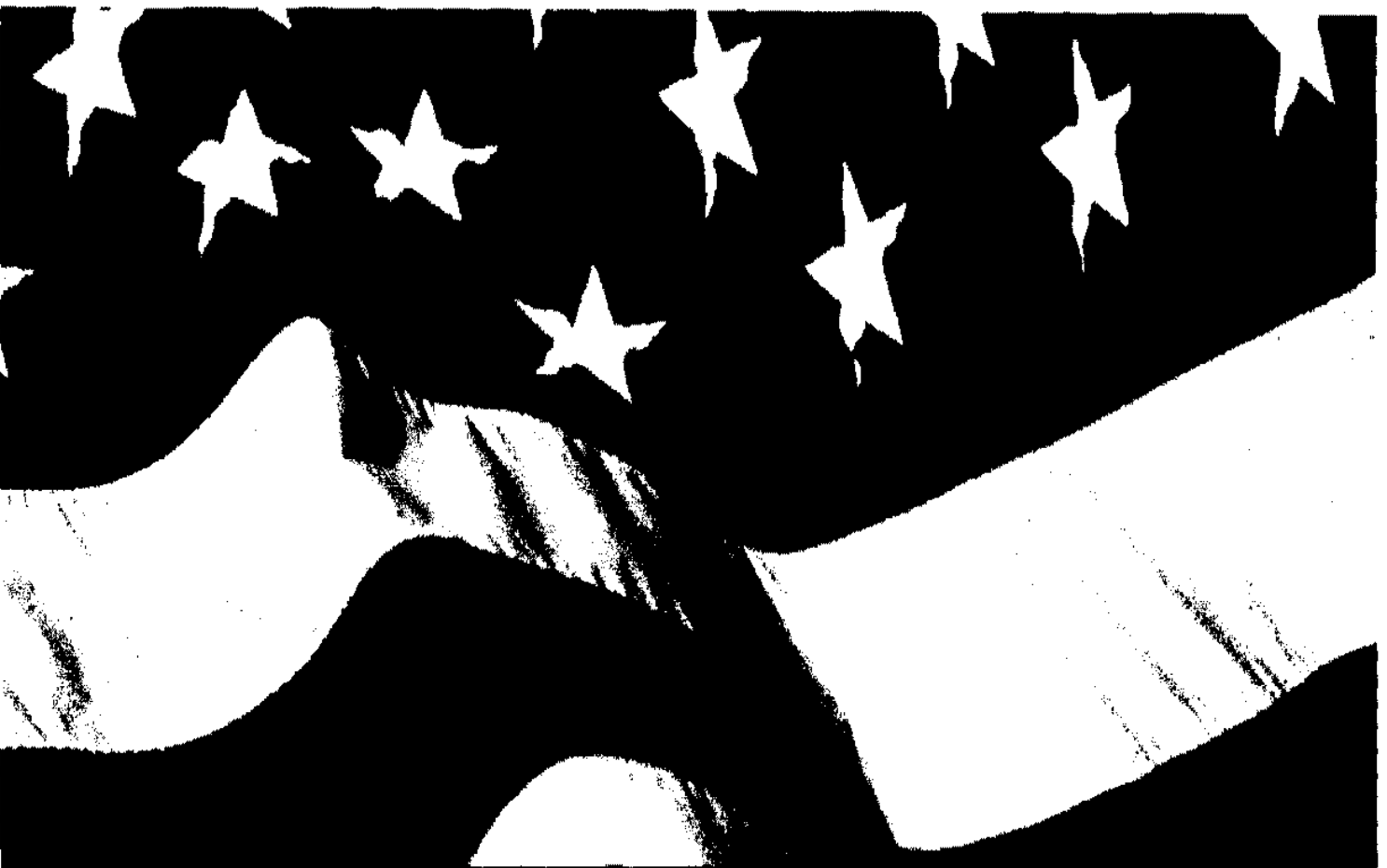
Appendix S. EBSP ARRA Milestones (continued)

Project Timelines – New Facility Modification Agreement Projects (continued)

Major Milestones	Estimated Completion Date
Colorado Springs Airport (COS)	
Notification letter sent to airport	July 2009
Draft OTA sent to airport to review the terms and conditions	July 2009
Airports submit updated cost information to TSA	late July 2009
Cost validations updated based on information provided by the airport	mid August 2009
Negotiation meetings scheduled with the airport	mid October 2009
Negotiations completed and OTA executed	January 2010
Little Rock National Airport (LIT)	
Notification letter sent to airport	July 2009
Draft OTA sent to airport to review the terms and conditions	July 2009
Airports submit updated cost information to TSA	late July 2009
Cost validations updated based on information provided by the airport	mid August 2009
Negotiation meetings scheduled with the airport	mid September 2009
Negotiations completed and OTA executed	November 2009
San Antonio International (SAT)	
Notification letter sent to airport	February 10, 2009
Draft OTA sent to airport to review the terms and conditions	March 22, 2009
Airports submit updated cost information to TSA	April 10, 2009
Cost validations updated based on information provided by the airport	April 17, 2009
Negotiation meetings scheduled with the airport	late May 2009
Negotiations completed and OTA executed	September 2009

FOR OFFICIAL USE ONLY

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.



In-line Explosives Detection Systems FTE Savings Fiscal Year 2010 Report to Congress

February 2010



Homeland
Security

Transportation Security Administration

Message from the Acting Administrator

I am pleased to present the following report, "In-line Explosives Detection Systems Personnel Savings," which has been prepared by the Transportation Security Administration (TSA). The report has been compiled in response to a directive in the Conference Report accompanying the Department of Homeland Security Appropriations Act, 2010, Public Law 111-83.

The report provides a summary of the federalized U.S. airports with in-line baggage handling systems and the associated full-time equivalent (FTE) savings that have resulted as a result of the installation of those systems.

Pursuant to congressional requirements, this report is being provided to the following Members of Congress:

The Honorable David E. Price
Chairman, House Appropriations Subcommittee on Homeland Security

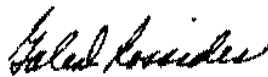
The Honorable Harold Rogers
Ranking Member, House Appropriations Subcommittee on Homeland Security

The Honorable Robert Byrd
Chairman, Senate Appropriations Subcommittee on Homeland Security

The Honorable George V. Voinovich
Ranking Member, Senate Appropriations Subcommittee on Homeland Security

Inquiries relating to this report may be directed to me at (571) 227-2801 or to the Department's Acting Chief Financial Officer, Peggy Sherry, at (202) 447-5751.

Sincerely,



Gale D. Rossides
Acting Administrator
Transportation Security Administration

Table of Contents

I. Legislative Requirement	1
II. Background	2
III. Data Report – FY 2009 FTE Savings	3
IV. Data Report – Projected FY 2010 FTE Savings.....	4

I. Legislative Requirement

The Conference Report which accompanied the Department of Homeland Security Appropriations Act, 2010, P.L. 111-83, included the following directive:

The conferees agree with the Senate recommendation to reduce funding below the request in this account due to repeated large carryover balances. With the large influx of funding provided by ARRA and this Act, TSA is able to greatly expedite the deployment of next generation technologies at the checkpoint and to install significantly more in-line explosives detection systems, thereby permitting a reduction in personnel. TSA shall report to the Committees, in tandem with the fiscal year 2011 budget, on the savings achieved and anticipated by fiscal year from the installation of the new systems. The report shall specifically address FTE savings.

II. Background

TSA identified which federalized airports possess In-line explosives detection systems (EDS) and the full-time equivalents (FTE) savings associated with the reduced staffing requirements resulting from the installation of those systems.

At the end of fiscal year 2009, a total of 52 airports possessed operational in-line EDS with an annual savings of 1,930 FTE versus their pre in-line equipment configuration. The data report in Section III provides a summary of these airports and their respective FTE savings. The airports listed represent locations where in-line systems are operational; however, some of those airports are still undergoing phased implementation and full FTE savings have not been fully realized.

Section IV provides a summary of FTE savings from in-line systems that are projected to become operational by the end of fiscal year 2010. It also includes airports from the FY09 list who have completed additional phases of in-line deployment. Savings for this period are projected to be 2,316 FTE. It is important to note that projected FTE savings associated with planned in-line systems are difficult to predict due to the multitude of variables which often delay these systems from becoming operational on schedule.

As previously briefed to the Appropriations Committee, FTE savings from in-line deployment have not reduced the overall FTE for the screening workforce. Savings have been reinvested in other security programs such as Ticket Document Checker, Aviation Direct Access Screening Program / Playbook, Behavior Detection Officers, and Bomb Appraisal Officers.

III. Data Report – FY 2009 FTE Savings

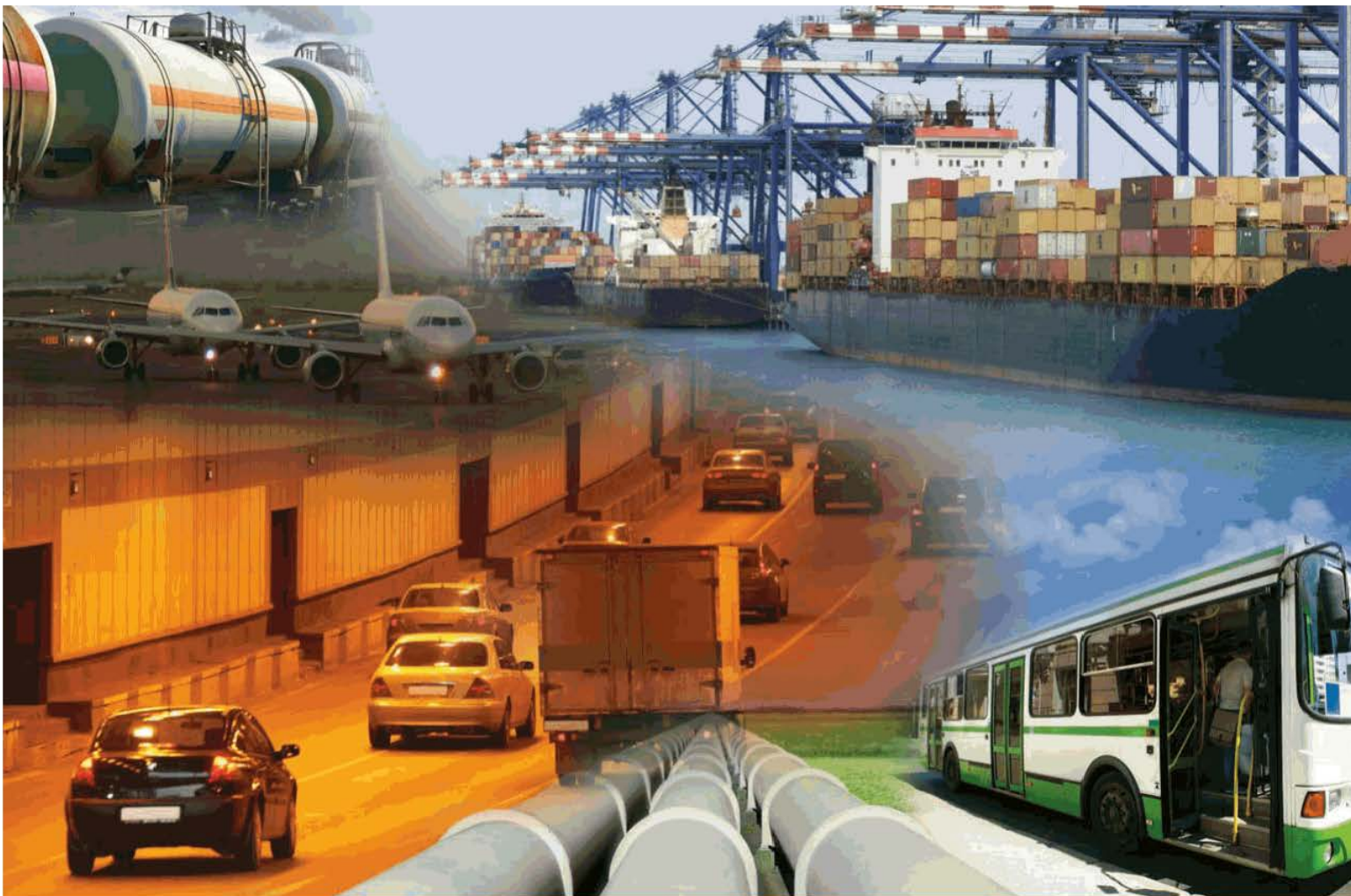
TSA INLINE BAGGAGE SCREENING AIRPORTS AND SAVINGS							
Airport ID	Airport Name	SAM04 FTE Savings	SAM05 FTE Savings	SAM06 FTE Savings	SAM07 FTE Savings	SAM08 FTE Savings	SAM09 FTE Savings
ANC	Ted Stevens Anchorage International	0.0	0.0	0.0	0.0	0.0	5.2
ATL	Hartsfield Atlanta International	0.0	0.0	0.0	96.5	96.5	96.5
AUS	Austin-Bergstrom International	0.0	0.0	0.0	7.5	45.0	45.0
BIS	Bismarck Municipal	0.0	0.0	0.0	1.3	2.5	3.8
BOI	Boise Air Terminal/Gowen Field	6.6	12.5	12.5	12.5	12.5	12.5
BOS	Logan International	95.7	95.7	95.7	95.7	95.7	95.7
BUF	Buffalo Niagara International	0.0	0.0	0.0	0.0	0.0	8.3
BUR	Burbank-Glendale-Pasadena	13.0	13.0	13.0	13.0	13.0	14.3
BWI	Baltimore-Washington International	0.0	0.0	0.0	21.1	21.1	21.1
CLE	Cleveland Hopkins International	0.0	0.0	0.0	5.5	11.0	11.0
DAL	Dallas Love Field	0.0	0.0	0.0	0.0	0.0	12.6
DEN	Denver International	0.0	46.0	91.8	91.8	91.8	91.8
DFW	Dallas/Fort Worth International	0.0	0.0	40.3	95.3	95.3	95.3
DTW	Detroit Metro Wayne County	0.0	0.0	20.3	20.3	20.3	20.3
EWR	Newark International	0.0	0.0	0.0	13.0	26.0	36.0
GEG	Spokane International	0.0	15.0	30.2	30.2	30.2	30.2
GSN	Salpan International	0.0	0.0	0.0	0.0	0.0	8.4
HNL	Honolulu International	0.0	0.0	0.0	7.5	30.0	40.0
HOU	William P. Hobby Houston	0.0	0.0	0.0	4.3	8.5	16.4
IAH	George Bush Intercontinental Houston	0.0	0.0	0.0	0.0	14.0	26.4
IND	Indianapolis International	0.0	0.0	0.0	0.0	0.0	33.8
JAX	Jacksonville International	0.0	0.0	12.0	23.2	23.2	23.2
JFK	John F. Kennedy International	0.0	0.0	0.0	0.0	40.0	40.0
LAS	McCarran International Las Vegas	0.0	0.0	44.0	66.0	66.0	120.1
MCI	Kansas City International	0.0	0.0	0.0	0.0	0.0	29.4
MCO	Orlando International	0.0	0.0	0.0	0.0	18.0	29.1
MDW	Chicago Midway	0.0	0.0	0.0	0.0	30.0	40.0
MHT	Manchester New Hampshire	10.0	19.1	19.1	19.1	19.1	19.1
MIA	Miami International	0.0	0.0	0.0	0.0	0.0	52.7
MSP	Minneapolis-St. Paul International	0.0	0.0	8.8	6.3	25.0	35.0
OAK	Metropolitan Oakland International	0.0	0.0	0.0	35.0	35.0	35.0
OGG	Kahului	0.0	0.0	0.0	0.0	3.4	3.4
OKC	Will Rogers World Oklahoma City	0.0	0.0	0.0	0.0	22.0	37.3
ONT	Ontario International	0.0	0.0	0.0	0.0	0.0	12.6
ORD	O'Hare International	0.0	0.0	0.0	24.0	40.0	68.0
PHL	Philadelphia International	0.0	0.0	0.0	0.0	25.0	25.0
PHX	Phoenix Sky Harbor International	0.0	0.0	0.0	0.0	20.0	42.0
PIT	Pittsburgh International	0.0	0.0	0.0	0.0	0.0	6.6
PVD	T F Green State Providence	0.0	0.0	0.0	0.0	0.0	5.9
RIC	Richmond International	0.0	0.0	0.0	15.0	30.0	30.0
RSW	Southwest Florida International	0.0	0.0	0.0	0.0	16.0	31.0
SAN	San Diego International	0.0	0.0	0.0	14.6	20.0	26.0
SDF	Louisville International	0.0	0.0	0.0	14.5	25.0	25.0
SEA	Seattle-Tacoma International	0.0	0.0	20.0	40.0	51.0	73.1
SFO	San Francisco International	0.0	100.0	170.0	170.0	170.0	170.0
SLC	Salt Lake City International	0.0	0.0	0.0	17.5	30.0	30.0
SMF	Sacramento International	0.0	0.0	0.0	0.0	11.2	11.2
SNA	John Wayne Santa Ana	16.0	32.1	32.1	32.1	32.1	32.1
SRQ	Sarasota Bradenton International	0.0	0.0	0.0	2.5	5.0	5.0
STL	Lambert St. Louis International	0.0	50.0	75.0	75.0	75.0	75.0
TPA	Tampa International	0.0	0.0	69.5	69.5	69.5	69.5
TYC	Cherry Capital Traverse City	0.0	0.0	0.0	2.1	4.2	4.2
TOTAL		141.2	383.4	754.3	1141.8	1539.1	1930.1

* SAM is the TSA reference to the Staffing Allocation Model process used to allocate resources to the airports.

IV. Data Report – Projected FY 2010 FTE Savings

TSA INLINE BAGGAGE SCREENING AIRPORTS AND SAVINGS								
Airport ID	Airport Name	SAM04 FTE Savings	SAM05 FTE Savings	SAM06 FTE Savings	SAM07 FTE Savings	SAM08 FTE Savings	SAM09 FTE Savings	SAM10 FTE Savings
ANC	Ted Stevens Anchorage International	0.0	0.0	0.0	0.0	0.0	5.2	27.2
ATL	Hartsfield Atlanta International	0.0	0.0	0.0	96.5	96.5	96.5	96.5
AUS	Austin-Bergstrom International	0.0	0.0	0.0	7.5	45.0	45.0	45.0
BIS	Bismarck Municipal	0.0	0.0	0.0	1.3	2.5	3.8	3.8
BOI	Boise Air Terminal/Gowen Field	6.5	12.5	12.5	12.5	12.5	12.5	12.5
BOS	Logan International	95.7	95.7	95.7	95.7	95.7	95.7	95.7
BUF	Buffalo Niagara International	0.0	0.0	0.0	0.0	0.0	8.3	8.3
BUR	Burbank-Glendale-Pasadena	13.0	13.0	13.0	13.0	13.0	14.3	14.3
BWI	Baltimore-Washington International	0.0	0.0	0.0	21.1	21.1	21.1	33.5
CLE	Cleveland Hopkins International	0.0	0.0	0.0	5.5	11.0	11.0	11.0
*CVG	Cincinnati/Northern Kentucky International	0.0	0.0	0.0	0.0	0.0	0.0	22.0
DAL	Dallas Love Field	0.0	0.0	0.0	0.0	0.0	12.6	12.6
DEN	Denver International	0.0	46.0	91.8	91.8	91.8	91.8	91.8
DFW	Dallas/Fort Worth International	0.0	0.0	40.3	95.3	95.3	95.3	95.3
*DSM	Des Moines International	0.0	0.0	0.0	0.0	0.0	0.0	5.5
DTW	Detroit Metro Wayne County	0.0	0.0	20.3	20.3	20.3	20.3	20.3
*ECP	Panama City Northwest Florida Beaches Int.	0.0	0.0	0.0	0.0	0.0	0.0	5.5
EWR	Newark International	0.0	0.0	0.0	13.0	26.0	36.0	36.0
GEG	Spokane International	0.0	15.0	30.2	30.2	30.2	30.2	30.2
GSN	Saipan International	0.0	0.0	0.0	0.0	0.0	8.4	8.4
HNL	Honolulu International	0.0	0.0	0.0	7.5	30.0	40.0	62.0
HOU	William P. Hobby Houston	0.0	0.0	0.0	4.3	8.5	16.4	16.4
IAH	George Bush Intercontinental Houston	0.0	0.0	0.0	0.0	14.0	26.4	37.4
IND	Indianapolis International	0.0	0.0	0.0	0.0	0.0	33.8	33.8
JAX	Jacksonville International	0.0	0.0	12.0	23.2	23.2	23.2	23.2
JFK	John F. Kennedy International	0.0	0.0	0.0	0.0	40.0	40.0	40.0
LAS	McCarran International Las Vegas	0.0	0.0	44.0	66.0	86.0	120.1	142.1
*LAX	Los Angeles International	0.0	0.0	0.0	0.0	0.0	0.0	64.6
MCI	Kansas City International	0.0	0.0	0.0	0.0	0.0	29.4	29.4
MCO	Orlando International	0.0	0.0	0.0	0.0	18.0	29.1	58.0
MDW	Chicago Midway	0.0	0.0	0.0	0.0	30.0	40.0	40.0
MHT	Manchester New Hampshire	10.0	19.1	19.1	19.1	19.1	19.1	19.1
MIA	Miami International	0.0	0.0	0.0	0.0	0.0	52.7	52.7
MSP	Minneapolis-St. Paul International	0.0	0.0	8.8	6.3	25.0	35.0	35.0
OAK	Metropolitan Oakland International	0.0	0.0	0.0	35.0	35.0	35.0	35.0
OGG	Kahului	0.0	0.0	0.0	0.0	3.4	3.4	15.8
OKC	Will Rogers World Oklahoma City	0.0	0.0	0.0	0.0	22.0	37.3	37.3
ONT	Ontario International	0.0	0.0	0.0	0.0	0.0	12.6	29.1
ORD	O'Hare International	0.0	0.0	0.0	24.0	40.0	68.0	68.0
PHL	Philadelphia International	0.0	0.0	0.0	0.0	25.0	25.0	36.0
PHX	Phoenix Sky Harbor International	0.0	0.0	0.0	0.0	20.0	42.0	102.5
PIT	Pittsburgh International	0.0	0.0	0.0	0.0	0.0	6.6	6.6
*PNS	Pensacola Regional	0.0	0.0	0.0	0.0	0.0	0.0	12.4
PVD	T F Green State Providence	0.0	0.0	0.0	0.0	0.0	5.9	5.9
RIC	Richmond International	0.0	0.0	0.0	15.0	30.0	30.0	30.0
*RNO	Reno/Tahoe International	0.0	0.0	0.0	0.0	0.0	0.0	33.0
RSW	Southwest Florida International	0.0	0.0	0.0	0.0	16.0	31.0	31.0
SAN	San Diego International	0.0	0.0	0.0	14.6	20.0	25.0	25.0
SDF	Louisville International	0.0	0.0	0.0	14.5	25.0	25.0	25.0
SEA	Seattle-Tacoma International	0.0	0.0	20.0	40.0	51.0	73.1	73.1
SFO	San Francisco International	0.0	100.0	170.0	170.0	170.0	170.0	170.0
*SJL	Luis Munoz Marin International	0.0	0.0	0.0	0.0	0.0	0.0	24.8
SLC	Salt Lake City International	0.0	0.0	0.0	17.5	30.0	30.0	30.0
SMF	Sacramento International	0.0	0.0	0.0	0.0	11.2	11.2	11.2
SNA	John Wayne Santa Ana	16.0	32.1	32.1	32.1	32.1	32.1	32.1
SRQ	Sarasota Bradenton International	0.0	0.0	0.0	2.5	5.0	5.0	5.0
STL	Lambert St. Louis International	0.0	50.0	75.0	75.0	75.0	75.0	75.0

TPA	Tampa International	0.0	0.0	69.5	69.5	69.5	69.5	69.5
TVC	Cherry Capital Traverse City	0.0	0.0	0.0	2.1	4.2	4.2	4.2
TOTAL		141.2	383.4	754.3	1141.8	1539.1	1930.1	2316.6
*Indicates airports with systems coming on line in FY 2010								



Transportation Systems Sector-Specific Plan

An Annex to the National Infrastructure Protection Plan

2010



Homeland
Security



Preface

The Transportation Security Administration (TSA) and the United States Coast Guard (USCG) are the Sector-Specific Agencies (SSAs) for the Transportation Systems Sector. TSA and the USCG, in collaboration with the Department of Transportation coordinate the preparedness activities among the sector's partners to prevent, protect against, respond to, and recover from all hazards that could have a debilitating effect on homeland security, public health and safety, or economic well-being.

This Transportation Systems Sector-Specific Plan (SSP) is the strategic plan for the sector fulfilling the requirements of Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection, and the requirements of the Intelligence Reform and Terrorism Prevention Act of 2004 (as amended) for the National Strategy for Transportation Security. The included modal annexes for mass transit and passenger rail, maritime, and freight railroads also consolidate strategic planning and infrastructure protection requirements.

The Transportation Systems SSP describes collaboratively developed strategies to reduce risks to critical transportation infrastructure from the broad range of known and unknown terrorism threats. The SSP adopts and amplifies the National Infrastructure Protection Plan risk management framework by describing a process intended to encourage wider participation in risk-reduction decisionmaking activities. The main objective of the process is to build a set of programs and initiatives that reduce the sector's most significant risks in an efficient, practical, and cost-effective manner. Examples of some of these programs and initiatives include:

- Achieved first milestone for screening cargo on passenger aircraft;
- Aligned transportation grant projects to reduce security risks in most vulnerable regions;
- Expanded sector security training and exercise program across all modes;
- Conducted 62 Area Maritime Security Plan exercises;
- Tracked the output measures of risk mitigation activities; and
- Developed key risk reduction programs such as Visible Intermodal Prevention and Response and Transportation Worker Identification Credential.

TSA, the USCG, and the sector partners will continue to work together to ensure continued progress toward the sector vision and goals through a broad set of risk mitigation activities (RMAs), such as those summarized above. Additional examples of how the SSAs collaborated with sector partners effectively to implement two major ongoing RMAs are:

- Transportation Worker Identification Credential (TWIC): A security program designed to ensure that individuals who pose a security threat do not gain unescorted access to secure areas of the nation's maritime transportation system. The credential is a biometric card that ensures only vetted workers can enter without an escort to secure transportation areas. The TWIC Program is jointly administered by TSA and the USCG.

- Intermodal Security Training and Exercise Program: A program that supports TSA's Transportation Sector Network Management Modal Security Managers and private sector partners with exercises and training. The program is designed to support all transportation security partners with security objectives and training that has clear and consistent performance measures.

The sector will review the SSP annually to make necessary updates or amendments. The SSAs look forward to working with sector partners to implement the risk management framework and improve the protection and resilience of the sector.

Each year, the Transportation Systems Sector Annual Report will provide updates on the sector's efforts to identify, prioritize, and coordinate the protection of its critical infrastructure, as defined in the Transportation Systems SSP. The Sector Annual Report provides the current priorities of the sector as well as the progress made during the past year in following the plans and strategies set out in the Transportation Systems SSP.



John P. Sammon

Chair, Transportation Systems Sector
Government Coordinating Council
Transportation Security Administration
U. S. Department of Homeland Security



Todd M. Keil

Assistant Secretary for Infrastructure Protection
U.S. Department of Homeland Security

Contents

Preface	i
Executive Summary	1
1. Sector Profile and Goal	1
2. Identify Assets, Systems, and Networks	4
3. Assess Risks	4
4. Prioritize Focus Areas	6
5. Develop and Implement Protective Programs and Resiliency Strategies	6
6. Measure Effectiveness	7
7. Research and Development	8
8. Managing and Coordinating SSA Responsibilities	10
Introduction	13
1. Sector Profile and Goals	15
1.1 Sector Profile	15
1.1.1 Sector and Cross-Sector Dependencies	16
1.1.2 Authorities	17
1.2 Sector Partners	17
1.2.1 Sector-Specific Agencies	18
1.2.2 The Sector Partnership Model	18
1.2.3 Other Federal Departments and Agencies	21
1.2.4 State, Local, Tribal, and Territorial Governments	22
1.2.5 Regional Coalitions	22
1.2.6 International Organizations and Foreign Governments	23
1.2.7 Private and Public Owners and Operators	23
1.3 Sector Goals and Objectives	24
1.4 Value Proposition	26
2. Identify Assets, Systems, and Networks	27
2.1 Defining Information Parameters	27
2.2 Collecting Infrastructure Information	28
2.3 Verifying and Updating Infrastructure Information	29
2.4 Critical Cyber Infrastructure Identification	29

3. Assess Risks	31
3.1 Use of Risk Assessment in the Sector	32
3.2 Assessing Sector Assets, Systems, and Networks	32
3.2.1 Featured Risk Assessment Methods	35
3.3 Assessing Consequences	37
3.4 Assessing Vulnerabilities	37
3.5 Assessing Threats	38
4. Prioritize Focus Areas	39
4.1 Intelligence and Risk Assessments	40
4.2 Legislative and Executive Requirements	40
4.3 Budget and Implementation Constraints	40
4.4 Safety and Privacy Considerations and Stakeholder Concerns	41
5. Develop and Implement Protective Programs and Resiliency Strategies	43
5.1 Overview of Sector Protective Programs and Resiliency Strategies	43
5.2 Determining the Need for Protective Programs and Resiliency Strategies	45
5.3 Selecting Protection and Resiliency Programs	45
5.4 Protective Program/Resiliency Strategy Implementation	46
5.5 Monitoring Program Implementation	47
6. Measure Effectiveness	49
6.1 Risk Mitigation Activities	50
6.2 Process for Measuring Effectiveness	51
6.2.1 Process for Measuring Sector Progress	51
6.2.2 Information Collection and Verification	52
6.2.3 Reporting	52
6.3 Using Metrics for Continuous Improvement	52
7. Research and Development	53
7.1 Overview of Sector R&D	53
7.1.1 Sector R&D Landscape	53
7.1.2 Sector R&D Partners	55
7.1.3 R&D Alignment with Sector Goals	55
7.2 Sector R&D Needs	56
7.2.1 Using the Capability Gap Process to Develop R&D Programs	56
7.2.2 Defining Sector R&D Needs	58
7.3 Sector R&D Plan	59

7.3.1 Components of the Sector R&D Plan	59
7.3.2 Sources of Input to the Sector R&D Plan	60
7.3.3 R&D Portfolio Framework	60
7.3.4 Technology Transition Through the R&D Life Cycle	61
7.4 Sector R&D Management Process	62
7.4.1 Sector R&D Governance	62
7.4.2 Sector R&D Working Group	63
7.4.3 Coordination with the Critical Infrastructure Protection R&D Community and Other Sectors	64
7.4.4 Progress and Impact of the Plan	64
7.4.5 Technology Scanning and Technology Transition	64
8. Managing and Coordinating SSA Responsibilities	65
8.1. Program Management Approach	65
8.2. Implementing the Sector Partnership Model (SPM)	66
8.3. Processes and Responsibilities	67
8.3.1 SSP Maintenance and Update	67
8.3.2 SSP Implementation Milestones	67
8.3.3 Resources and Budgets	68
8.3.4 Training and Education	69
8.3.5 Compliance and Assessment Processes	69
8.3.6 Intermodal Protection Process	69
8.3.7 Response and Recovery	70
8.3.8 Lessons-Learned Process	70
8.4 Information Sharing and Protection	70
Appendix 1: Acronym List	73
Appendix 2: Glossary of Terms	81
Appendix 3: Transportation Systems Sector Authorities	85
Appendix 4: Transportation Systems Sector Partners	91
Appendix 5: The Capability Gap Process	99
Appendix 6: Taxonomy	105
Modal Annexes	121
Annex A: Aviation	123

Annex B: Maritime	165
Annex C: Mass Transit and Passenger Rail	207
Annex D: Highway Infrastructure and Motor Carrier	245
Annex E: Freight Rail	277
Annex F: Pipeline	311

List of Figures

Figure 1-1: Transportation Systems Sector GCC Organization	19
Figure 1-2: Transportation Systems SCC Organization	20
Figure 1-3: Transportation Systems Sector Risk Management Framework	24
Figure 3-1: Three Classes of Risk Assessments	34
Figure 3-2: TSSRA's Information Collection Process	36
Figure 4-1: Inputs into the Development of Protection and Resiliency Priorities	40
Figure 5-2: Layered Approach to Aviation Security	46
Figure 7-1: Capability Gap Process	57
Figure 7-2: Transportation Systems Sector R&D Plan Process	60
Figure 7-3: Technology Transition Through the R&D Life-Cycle	62
Figure 7-4: Interconnected Transportation Systems Sector R&D Community Relationships	63
Figure 8-1: Transportation Systems Sector Management Approach	65
Figure 8-2: Implementing the Sector Partnership Model	66
Figure A5-1: Capability Gaps Process	99
Figure A5-2: Capability Gap Form	102
Figure A5-3: Capability Gap Bucket Criteria	104

List of Tables

Table 1-1: Transportation Systems Sector Modal Divisions	15
Table 5-1: Transportation System Sector Risk Mitigation Activities	44
Table 6-1: Transportation Sector Risk Mitigation Activities Mapped to Sector Goals	50
Table 6-2: Maritime Mode Risk Mitigation Activities Mapped to Sector Goals	51
Table 7-1: R&D Security Needs by Transportation Infrastructure Element	54
Table 7-2: Alignment of Sector Goals and R&D Objectives	55
Table 8-1: SSP Risk Management Milestones and Way Forward	67
Table A5-1: Capability Workgroup Participants	100
Table A5-2: Capability Gaps to Risk Relationships	103

Executive Summary

The Transportation Systems Sector-Specific Plan (SSP) is the strategic plan for the sector fulfilling the requirements of Homeland Security Presidential Directive 7 (HSPD-7): Critical Infrastructure Identification, Prioritization, and Protection; and the requirements of the Intelligence Reform and Terrorism Prevention Act of 2004 (as amended by the 9/11 Commission Act)¹ for the National Strategy for Transportation Security (NSTS). The SSP consists of a base plan and six modal annexes. The modal annexes for mass transit, maritime, and railroads (including freight and passenger rail) also consolidate strategic planning and infrastructure protection requirements.

The Transportation Systems SSP describes collaboratively developed strategies to reduce risks to critical transportation infrastructure from the broad range of known and unknown terrorism threats. These threats span a multitude of scenarios from lone actors with explosives devices to complex and coordinated assaults such as the 9/11 attack or, potentially, attacks involving weapons of mass destruction. The SSP establishes the strategic goals and objectives to be implemented in order to achieve a shared vision of a safe and secure national transportation system and it explains processes and mechanisms to manage sector risks.

The 2010 SSP revises the Systems-Based Risk Management process described in the 2007 version of the SSP, and adopts and amplifies the National Infrastructure Protection Plan (NIPP) framework by describing a process intended to encourage wider participation in risk reduction decisionmaking activities. The main objective of the process is to build a set of programs and initiatives that reduce the sector's most significant risks in an efficient, practical, and cost-effective manner.

The Transportation Security Administration (TSA) and the United States Coast Guard (USCG) are the Sector-Specific Agencies (SSAs) for the Transportation Systems Sector. TSA and the USCG, in collaboration with the Department of Transportation (DOT), coordinate the preparedness activities among the sector's partners to prevent, protect against, respond to, and recover from all hazards that could have a debilitating effect on homeland security, public health and safety, or economic well-being.

1. Sector Profile and Goal

The Nation's transportation network is an expansive, open, and accessible set of interconnected systems of airways, roads, tracks, terminals, and conveyances that provide services essential to our way of life. The sector includes six, interconnected subsectors or modes—aviation, freight rail, highway, maritime, mass transit and passenger rail, and pipelines—that transport people, food, water, medicines, fuel, and other commodities vital to the public health, safety, security, and economic well-being of our Nation. The sheer size and capacity of the sector, which moves, distributes, and delivers billions of passengers and

¹ Enacted by the Intelligence Reform and Terrorism Prevention Act, P.L. 108-458, § 4001, (2004), as amended by the Implementing Recommendations of the 9/11 Commission Act, P.L. 110-53, § 1202 (2007).

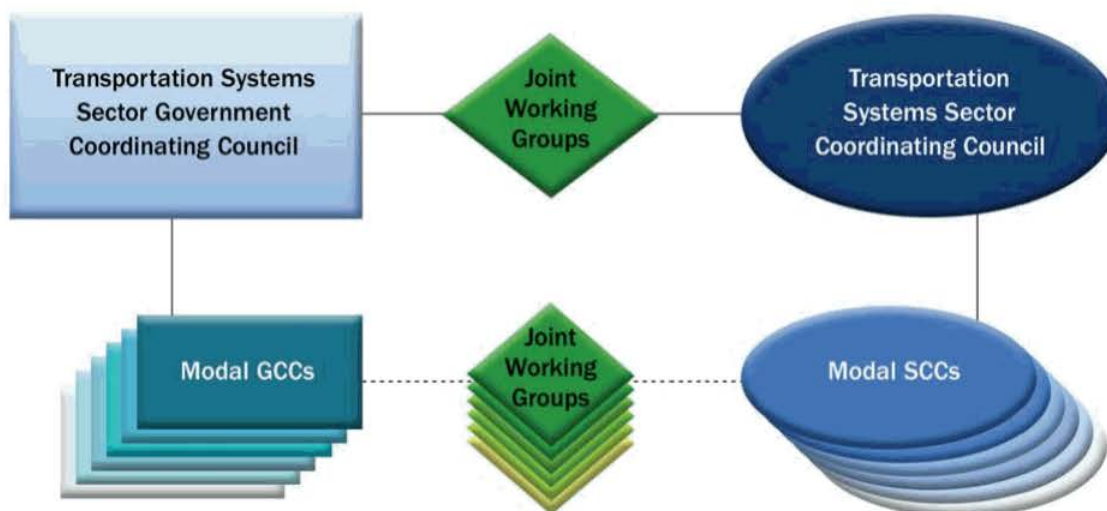
millions of tons of goods each year, makes it a highly attractive target for terrorists, as well as vulnerable to all types of man-made and natural disasters.

The vast majority of the transportation infrastructure in the United States is owned by the private sector. Infrastructure is composed of physical, human, and cyber components working together to provide transportation services. The 2010 SSP encourages greater awareness of the codependent nature of the components when assessing infrastructure risks. Emphasis is placed on improving assessments of the cyber component and vulnerabilities that may impact critical infrastructure operations or the transportation systems as a whole.

All of the critical infrastructure sectors depend on transportation services, and conversely, the Transportation Systems Sector depends on the Energy, Communications, Information Technology, Chemical, and Critical Manufacturing Sectors. Interdependencies are an important dimension of the risk environment that must be considered to protect critical infrastructure and achieve system resiliency.

The Transportation Systems Sector Partnership Model (SPM) consists of Government Coordinating Councils (GCCs) as indicated in the diagram below, and a parallel set of Sector Coordinating Councils (SCCs) shown in Chapter 1. The GCCs members are representatives of government organizations and the SCCs include representatives of the transportation industry. The GCCs and SCCs communicate with one another regarding infrastructure risk assessments, planning, prioritization, programming, and risk reduction measurement. Several joint working groups provide for direct collaboration on specific infrastructure protection and resiliency issues.

Implementing the Sector Partnership Model



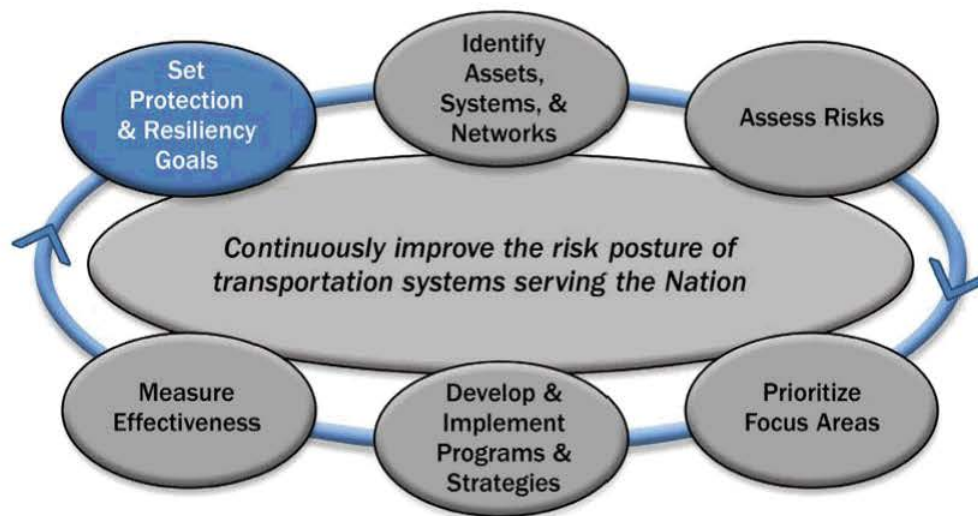
International partnerships are essential to achieve the transportation protection and resiliency objectives. TSA, the USCG, and the Department of State strive to assure that foreign governments and foreign air carriers and transportation companies meet international security protocols and that international standards satisfy U.S. security concerns. Strengthening transportation protection across all modes of the global transportation network requires extensive, world-wide collaboration with groups such as: the European Union (EU); the Group of Eight members; the Asia-Pacific Economic Cooperation Forum; the International Civil Aviation Organization; the International Maritime Organization; and the Organization of American States. In addition to strengthening partnerships with established groups, the SSAs, engage in bilateral and multilateral partnerships with key international partners to include Canada, the EU, Israel, Japan, Mexico, and Australia.

Since the majority of transportation infrastructure is operated by privately or publicly owned companies, participation of infrastructure owners and operators in protection and resilience planning, risk management, and measurement is a cornerstone of the SSP.

In the wake of the attacks of September 11, 2001, many trade associations developed or enhanced security operations to deal with terrorist threats. Numerous owners and operators of transportation infrastructure and the representative associations provide technical expertise during the development of best practices, voluntary standards, and regulations. The sector continues to rely on the expertise of owners and operators of critical transportation infrastructure to understand risks and to determine the most appropriate and cost-effective means to reduce risks.

The sector's goals and objectives align with the President's homeland security agenda, DHS priorities, and statutory mandates for protecting the transportation system and improving resiliency of critical infrastructure. These goals and objectives shape the approach for managing sector risk. The risk management framework depicted below is described in chapters 2 through 6.

Transportation Systems Sector Risk Management Framework



The sector's vision statement describes: *A secure and resilient transportation system, enabling legitimate travelers and goods to move without significant disruption of commerce, undue fear of harm, or loss of civil liberties.*

The sector's mission is to: *continuously improve the risk posture of transportation systems serving the Nation.*

Four goals have been developed to guide activities to accomplish the mission:

- Goal 1:** Prevent and deter acts of terrorism using, or against, the transportation system;
- Goal 2:** Enhance the all-hazard preparedness and resilience of the global transportation system to safeguard U.S. national interests;
- Goal 3:** Improve the effective use of resources for transportation security; and
- Goal 4:** Improve sector situational awareness, understanding, and collaboration.

2. Identify Assets, Systems, and Networks

Critical infrastructure includes those assets, systems, and networks, which if damaged, could result in significant consequences—adverse impacts on national economic security, national public health and safety, public confidence, the environment, loss of life, or some combination of these. The primary method for identifying the sector’s critical infrastructure is the annual National Critical Infrastructure Prioritization Program (NCIPP). NCIPP is managed by DHS and provides a standardized approach for sectors to determine criticality of assets, systems, and cyber components.

The determination of criticality relies on the availability of asset data and valuations of consequences for specific hazard scenarios. Much of the data reside with transportation companies, therefore, owners and operators have an important role in the process. Infrastructure data are stored in the DHS Infrastructure Data Warehouse (IDW) and are used to assess risk within and across sectors and to develop incident management and recovery plans for natural disasters.

3. Assess Risks

Two types of risks are considered in assessments: risks to the transportation system and risks from the transportation system, e.g., attacks using transportation assets against another target. Assessments inform decisions regarding priorities, programs, and budgets for reducing those risks.

Risks of natural disasters can be determined based on the likelihood of the disaster and the anticipated consequences.

$$\text{Risk} = f(\text{Probability, Consequence})$$

Terrorist risks do not have a statistical basis for determining probability; therefore, the following alternate equation, developed by the Government Accountability Office in 2001, is typically used within the sector:

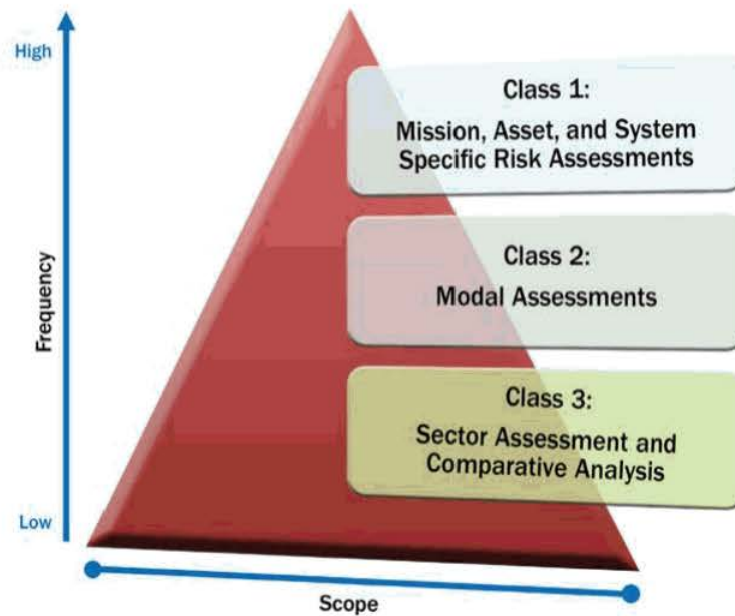
$$\text{Risk} = f(\text{Threat, Vulnerability, Consequence})$$

The assessment of risks to transportation infrastructure is complicated by the:

- Uncertainty as to the types of threats;
- Difficulties of predicting the likelihood and consequences of known risks;
- Inestimable nature of unknown risks;
- Unique differences between risk assessments for manmade incidents (including terrorism) versus natural disasters;
- Creative and adaptive nature of terrorists; and
- Widely varying preparedness and response capabilities and countermeasures within the groups and subgroups of modal infrastructure.

Three types or classes of assessments, as depicted below, have evolved within the sector and can be broadly characterized as Mission, Asset, and System Specific Risk Assessments (MASSRA), modal risk assessments, and sector cross-modal risk assessments.

Three Classes of Risk Assessments



Class 1 assessments, or MASSRA, focus on one or more of the risk elements or on scenario-specific assessments (for example, a blast effect analysis on a certain type of conveyance). Physical security self-assessments conducted by transportation service providers that estimate vulnerability are within the MASSRA category. These assessments generally do not cross jurisdictional lines and have a narrow, specific focus.

Class 2 assessments are modal risk assessments used to identify how best to determine high-risk focus areas within a mode of transportation. These assessments also help to establish the sector's priorities for a specific mode.

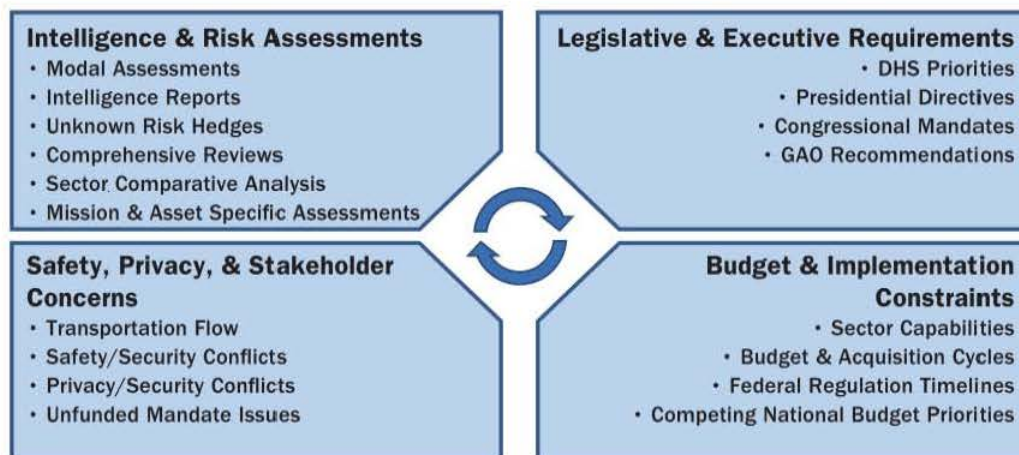
Class 3 assessments are cross-modal comparative analyses focusing on two or more modes, or on the entire sector. These analyses help identify strategic planning priorities and define long-term visions. Cross-modal analyses inform key leadership decisions and policies, including investments in countermeasures.

Assessments may focus on a single risk factor or consider all three: threat, vulnerability, and consequence. Threat assessments typically rate an adversary's capability and intent to execute a particular attack scenario. Consequence assessments consider one or more of the following: repair or reconstruction costs; health and human safety; economic impact; national security; and cross-sector effects. Vulnerability assessments determine the weakness in the physical, cyber, human, or operational aspects of the infrastructure that render it open to exploitation or susceptible to hazards.

4. Prioritize Focus Areas

Assessment information is analyzed in combination with other factors in the decision environment, to enable the sector to set risk reduction priorities. The prioritization process leads to strategic priorities for the sector with implications for resource distribution and budget submissions. The figure below depicts examples of the factors that the sector considers when developing priorities and strategies.

Inputs into the Development of Protection and Resiliency Priorities



A degree of uncertainty concerning risk, particularly regarding terrorism is always present. Unknown risk results from the virtually limitless range of targets and tactics available to terrorists. Terrorists are adaptive and shift tactics and strategies in reaction to, or in anticipation of, countermeasures. While the sector remains focused on known and suspected threats, it also must address risks associated with unknown threats.

Key to improving transportation resiliency is striking a balance between countering known risks and hedging against unknown risks. Currently, these hedges involve two strategies: deploying random security countermeasures and enhancing system resiliency to all hazards. One approach used in the sector to address unknown risk is through random, flexible, deterrent initiatives, such as Visible Intermodal Prevention Response (VIPR) teams.

5. Develop and Implement Protective Programs and Resiliency Strategies

The sector partners analyze risk assessments to determine security and resiliency priorities and to develop, implement, and measure protective programs and resiliency strategies. Protective programs are intended to reduce risks from all types of hazards by detecting and deterring threats, preparing for known threats, increasing the sector's overall resiliency, and enhancing readiness for continuity and recovery operations. In many cases, multiple programs and strategies are layered to reduce the overall risk by mitigating vulnerabilities and reducing consequences in the event of an incident. Other programs have been developed to address evolving threats. As programs are developed and implemented by various sector partners, they are monitored to ensure continuous improvement.

The strategies for addressing particular vulnerabilities include proposals for grants, research and development, training, structural improvements, security equipment procurement, personnel policy changes, and a variety of other possible strategies. The consequences attributed to a threat are diminished by changing vulnerabilities identified in the assessment. Similarly, threats can be reduced by addressing the vulnerabilities that allow threats to succeed. Therefore, it is important to link vulnerabilities

identified in assessments or subsequent analyses to the risk-reduction programs under consideration. A variety of analytical methods are available to reach a decision among risk reduction alternatives. The Transportation Systems SSA recommends using a weighted-factor decision method to evaluate programming alternatives to reduce risks.

When capability gaps are identified in the assessments, the strategy may be to seek research, development, modeling, and simulation support to address ways to close the gaps. The joint Transportation Systems Sector Research and Development Working Group (R&DWG) determines research and development (R&D) priorities, establishes programming recommendations, and monitors implementation of those programs.

Cyber vulnerabilities identified for remediation are the responsibility of the agency or owner and operator. The SSAs coordinate participation in these programs through the sector's GCCs and SCCs and with the National Cyber Security Division (NCSD). The Transportation Systems Sector Cyber Working Group monitors implementation of cyber risk reduction programs for alignment across agencies and the sector.

6. Measure Effectiveness

Performance metrics are an important step in the risk management process that enables the sector to objectively assess the reduction of risks associated with infrastructure protection and resiliency efforts. Performance metrics allow progress to be tracked against sector priorities and provide a basis for the sector to provide feedback to decisionmakers.

The Transportation Systems SSA and Maritime SSA risk mitigation activity (RMA) categories represent the strategic focus areas for risk reduction, under which individual, cross-modal, and sector-wide programs and initiatives are aligned. The RMAs support the sector's goals and objectives as indicated in the following tables.

The sector plans to measure the effectiveness of security programs and initiatives by comparing their results against established baselines within the RMA categories. Baselines are specific to each type of program or initiative; for example, a baseline measure for VIPR team effectiveness is inherently different than one for an electronic boarding pass program. Despite the inherent differences, comparisons between activities may be made by determining deviations from the baseline as a percentage of change, or improvement attributed to the activity.

Key Transportation SSA RMA	Goal to which Activity Maps			
	Goal 1	Goal 2	Goal 3	Goal 4
Security vetting of workers, travelers, and shippers	✓		✓	
Securing of critical physical infrastructure	✓	✓		✓
Implementation of risk mitigating operational practices	✓	✓	✓	✓
Implementation of unpredictable operational deterrence	✓		✓	✓
Screening of workers, travelers, and cargo	✓	✓	✓	
Security awareness and response training	✓	✓		✓
Preparedness and response exercises	✓	✓		✓
Awareness and preparedness	✓	✓	✓	✓

Key Transportation SSA RMA	Goal to which Activity Maps			
	Goal 1	Goal 2	Goal 3	Goal 4
Leveraging of technologies	✓	✓	✓	
Transportation industry security planning	✓	✓	✓	✓
Vulnerability assessments	✓	✓	✓	✓
Securing of critical cyber infrastructure	✓	✓		✓

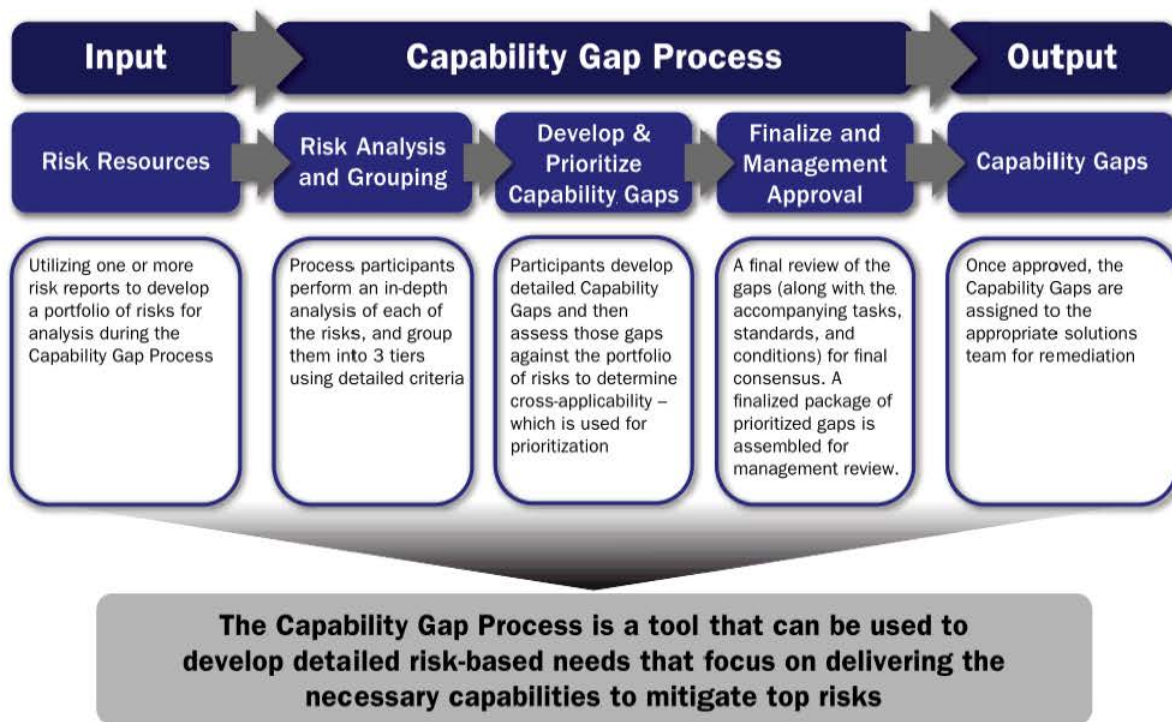
Key Maritime SSA RMA	Goal to which Activity Maps			
	Goal 1	Goal 2	Goal 3	Goal 4
Maritime Domain Awareness	✓		✓	
Risk reduction tools and methods		✓	✓	✓
Create and oversee an effective maritime security regime	✓	✓	✓	
Lead and conduct effective maritime and security response operations		✓	✓	✓

7. Research and Development

The Transportation Systems Sector R&DWG brings stakeholders from across the sector together to identify mission needs and capability gaps. These needs and gaps are eventually forwarded into the DHS Science and Technology (S&T) Capstone Integrated Project Team Process, which allows multiple DHS constituents to collaborate to develop programs and projects that close capability gaps and expand related mission competencies.

The Capability Gap Process in the figure below allows the sector to identify and prioritize capability gaps that limit its ability to achieve the mission. These gaps are typically determined by the modal stakeholders based on risk assessments and their analyses. Vulnerabilities indicated in the assessments are submitted to the R&DWG. Through a series of analytical steps, the working group develops a capability gap statement that contains the required information and justifications for consideration by DHS for R&D funding. The results of this process are recorded in the Sector Annual Report (SAR) which informs DHS for development of the annual National Critical Infrastructure Protection Research and Development Plan (NCIP R&D Plan).

Capability Gap Process



The NCIP R&D Plan is structured around the nine R&D themes that support all 18 critical infrastructure sectors and reflect the concerns of infrastructure owners and operators, industry representatives, and government officials:

- Detection and Sensor Systems
- Protection and Prevention
- Entry and Access Portals
- Insider Threats
- Analysis and Decision Support Systems
- Response and Recovery Tools
- New Emerging Threats
- Advanced Infrastructure Architectures and System Designs
- Human and Social Issues

Risk-based technology requirements for the sector are grouped in the following broad categories discussed in greater detail in chapter 7:

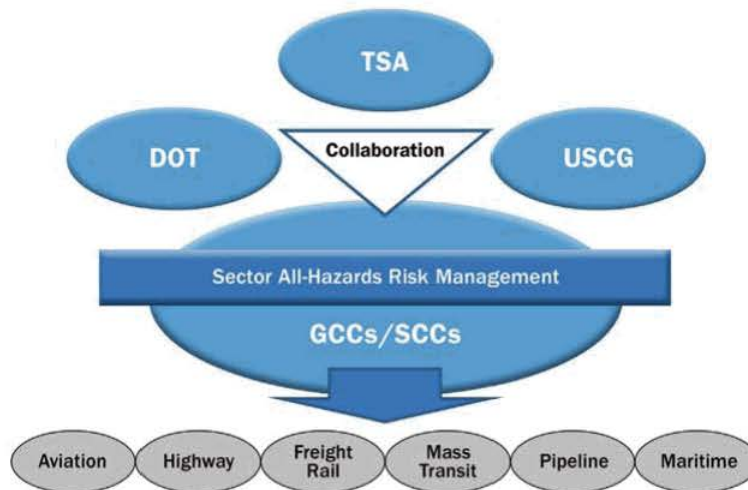
- Enhance screening effectiveness for passengers, baggage, cargo, and materials for the six modes of transportation within the sector;
- Enhance infrastructure and conveyance security;
- Improve information gathering and analysis;

- Provide a common operating picture for transportation systems; and
- Implement needed cybersecurity capabilities.

8. Managing and Coordinating SSA Responsibilities

The sector's SSAs share the responsibility for overseeing and coordinating the implementation of the SSP and the modal plans. The figure below provides a conceptual view of the relationships between the SSAs and the GCCs and SCCs. The sector-wide and modal GCCs and SCCs and their working groups are the primary means for collaboration among the sector partners to implement the SSP.

Transportation Systems Sector Management Approach



Several modes have active advisory committees that also provide security advice to Federal managers. Other modal partnership forums provide a regional voice for security concerns. For example, the Maritime SSA uses the Area Maritime Security Committees within each Captain of the Port Zone to collaborate with stakeholders in the port.

Joint working groups chartered under the Critical Infrastructure Partnership Advisory Committee have been established for collaboration regarding cross-modal research and development and cybersecurity. Joint working groups are being considered for risk assessments and analyses, information sharing, and metrics.

The SSAs are responsible for coordinating GCC and SCC participation in annual reviews and updates of the plan and the development of the annual progress reports to DHS. The SAR contributes to the development of the Critical Infrastructure and Key Resources (CIKR) Protection National Annual Report (NAR) and is one of 18 SARs appended to the NAR. The NAR is submitted to the White House and to Congress. Among other things, the SAR reports on progress in meeting the objectives in the SSP, indicated below.

SSP Risk Management Milestones and Way Forward

Risk Management Framework	Milestones (in light blue)
	Way Forward (in dark blue)
Set Protection & Resiliency Goals	<ul style="list-style-type: none"> • Conduct annual review and validation/update based on process feedback • Update modal cybersecurity objectives for modal specific and intermodal concerns
	<ul style="list-style-type: none"> • Communicate goals and objectives to the sector • Sponsor voluntary establishment of a sector-level SCC • Review transportation goals and objectives of State homeland security advisors and other jurisdictions during SSP review process
Identify Assets, Systems, & Networks	<ul style="list-style-type: none"> • Participate in annual DHS National Critical Infrastructure Prioritization Program and the Critical Foreign Dependencies Initiative
	<ul style="list-style-type: none"> • Refine the sector CIKR identification process to include recognition of critical cyber systems • Establish criteria for considering intermodal consequences in identifying critical infrastructure • Encourage owners and operators to provide asset information to sector infrastructure databases
Assess Risks	<ul style="list-style-type: none"> • Refine the sector strategic risk assessment model for the annual risk assessment requirement
	<ul style="list-style-type: none"> • Develop modal risk assessment models for critical cyber systems • Define data elements for the sector data repository to support risk assessments • Incorporate sector compliance and assessment data into sector database
Prioritize Focus Areas	<ul style="list-style-type: none"> • Update priorities based on annual assessments
	<ul style="list-style-type: none"> • Develop processes for analysis and prioritization of cyber risks • Develop process to determine protection and resiliency lessons-learned during incidents and to apply them to prioritization decisions
Develop & Implement Programs & Strategies	<ul style="list-style-type: none"> • Update the Transportation Systems Information Sharing Plan annually • Consult non-profit employee representative organizations regarding the SSP • Incorporate all-hazards considerations in capability gap analyses
	<ul style="list-style-type: none"> • Improve participation of agencies and sector partners in the Transportation Systems Sector R&DWG • Establish the Transportation Security ISAC • Increase awareness of criticality of cyber systems to transportation operations • Conduct pilot of cybersecurity risk management approach
Measure Effectiveness	<ul style="list-style-type: none"> • Work with government partners and DHS IP to meet the NIPP's annual metrics milestones
	<ul style="list-style-type: none"> • Develop data streams to determine risk reduction effectiveness of protection and resiliency programs • Participate in the SAR process

Each of the sector's partners contributes to resourcing the activities that address the protection and resiliency objectives for transportation systems. As priorities are determined and risk reduction options are considered, the SSAs discuss threats and vulnerabilities with stakeholders through the partnership framework, determine priorities, and apportion resources to effectively address those priorities.

The Federal resources include field personnel for screening, inspections, compliance audits, assessments, law enforcement, and explosive detection (e.g., canine units). Federal funding is available to sustain protection and resiliency related programs and operations through appropriations or through grants to the States or to transportation entities. FEMA also funds Federal, State, territorial, tribal, and local entities during declared emergencies for expenses exceeding normal mission responsibilities and budgets. Additional homeland security grant funds are available for first responders and other response and recovery preparedness activities in States, localities, and tribal areas. DOT also administers a number of grant programs for infrastructure improvements that often benefit the homeland security mission through hardening or other means that create more resilient structures or operations.

The owners and operators of the sector's critical assets, systems, and networks bear a large share of the protection and resiliency responsibilities and contribute extensively to homeland security activities. Consequently, the sector strives to minimize costs while maximizing benefits of risk management activities necessary to protect infrastructure, people, and cargo, and to enhance system resiliency.

Risks associated with the interface between modes require special consideration. Intermodal risks occur where the infrastructure of several modes converge, such as transit terminals, bridges, or tunnels; or where goods being transported by one mode are transferred to another. Intermodal risks are being addressed through training and education, drills and exercises, assessments and compliance activities, unpredictable deterrent activities, R&D, risk analyses and modeling, information sharing, and response and recovery planning.

Introduction

The Transportation Systems Sector-Specific Plan (SSP) is one of the 18 sector-specific plans required by the National Infrastructure Protection Plan (NIPP) and Homeland Security Presidential Directive 7 (HSPD-7).² The NIPP requirements and the National Strategy for Transportation Security (NSTS) requirements are combined into the SSP as a single strategic plan. Consistent with the provisions of 49 U.S.C. 114 (s)³ to synthesize Federal strategy and planning efforts, the integrated SSP governs Federal transportation security efforts. Both the NSTS and the SSP cover similar content, require collaborative development, and have annual reporting requirements. Consequently, in combining these two strategic documents, the Transportation Systems Sector (sector) achieves significant efficiencies for its security partners and minimizes the potential for out-of-date or conflicting information due to the different revision cycles for each document.

Several modal annexes to the SSP combine national strategies required under legislative or executive mandates. The National Maritime Transportation Security Plan, the National Strategy for Railroad Security, and the National Strategy for Public Transportation Security are incorporated into the respective Maritime, Freight Rail, and Mass Transit and Passenger Rail modal annexes. The National Strategy for Aviation Security is not replaced by the Aviation Annex to this Plan; however, they are aligned.

Under HSPD-7, the Nation's critical infrastructure and key resources (CIKR) are organized into 18 sectors with certain Federal agencies designated as Sector-Specific Agencies (SSAs). These agencies are responsible for coordinating the preparedness and resiliency activities among the sectors' partners to prevent, protect against, respond to, and recover from threats that could have a debilitating effect on homeland security, public health and safety, economic well-being, or any combination of these. The sector faces a broad range of threats which span a multitude of scenarios from lone actors with weapons or explosive devices to complex and coordinated assaults such as the 9/11 attack or, potentially, attacks involving weapons of mass destruction.

The Secretary of Homeland Security designated the Transportation Security Administration (TSA) and the United States Coast Guard (USCG) as the SSAs for the Transportation Systems Sector. The SSAs, in collaboration with the Department of Transportation (DOT) and other Federal, State, local, tribal, territorial, and private industry partners, share the responsibility for developing, implementing, and updating the SSP. The SSP addresses the counterterrorism preparedness requirements of the various national strategies and also risk mitigation associated with all hazards. Examples of disruptive incidents include terrorist attacks, forest fires, tanker explosions, Spills of National Significance (SONS), hurricanes, and floods. Counterterrorism preparedness activities frequently have protection and resiliency effects that reduce risks associated with natural and accidental threats. Perhaps more significantly, response and recovery activities—already well developed under the National Response

² Homeland Security Presidential Directive 7 (HSPD-7), Critical Infrastructure Identification, Prioritization, and Protection (December 17, 2003).

³ Enacted by the Intelligence Reform and Terrorism Prevention Act, P.L. 108-458, § 4001, (2004), as amended by the Implementing Recommendations of the 9/11 Commission Act, P.L. 110-53, § 1202 (2007).

Framework and procedures established by Federal Emergency Management Agency (FEMA) and by DOT—rely on common resources and capabilities associated with emergency management of all hazards.

The NIPP provides a risk management framework indicating the basic steps for reducing risks to assets, systems, and networks. The 2010 SSP revises the Systems-Based Risk Management process described in the 2007 version of the SSP, and adopts and amplifies the NIPP framework by describing a process which encourages sector partner participation in risk reduction decision-making activities. The main objective of the process is to build a set of activities that reduce the sector's most significant risks in an efficient, practical, and cost-effective manner.

This plan does not alter or impede the ability of Federal departments and agencies to perform their responsibilities under law. This plan does not create any right or benefit, substantive or procedural, enforceable by law or in equity, against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.

1. Sector Profile and Goals

1.1 Sector Profile

The Nation's transportation network is an expansive, open, accessible, interconnected system, with the vast majority of the transportation infrastructure in the United States owned by the private sector. In addition to physical infrastructure, the sector's cyber assets continue to gain importance in terms of ensuring the integrity and continuity of business operations. The sheer size and capacity of the sector, which moves, distributes, and delivers billions of passengers and millions of tons of goods each year, makes it a highly attractive target for terrorists, as well as vulnerable to all types of manmade and natural disasters.

The sector is comprised of six interconnected subsectors or modes—aviation, freight rail, highway, maritime, mass transit and passenger rail, and pipelines—that transport people, food, water, medicines, fuel, and other commodities vital to the public health, safety, security, and economic well-being of our Nation. An overview of the six modes of transportation is presented in table 1-1 below. A more detailed list of the modes' assets is included in Appendix 6–Taxonomy.

Table 1-1: Transportation Systems Sector Modal Divisions

Aviation	Composed of aircraft, air traffic control systems, and approximately 450 U.S. commercial airports and 19,000 additional public airfields. This mode includes civil and joint-use military airports, heliports, short takeoff and landing ports, and seaplane bases.
Freight Rail	Consists of seven major carriers, hundreds of smaller railroads, over 140,000 miles of active railroad, over 1.3 million freight cars, and roughly 20,000 locomotives. Over 12,000 trains a day are operating. The Department of Defense has designated 30,000 miles of track and structure as critical to mobilization and resupply of U.S. forces.
Highway and Motor Carriers	Encompasses more than four million miles of roadways and associated infrastructure such as 600,000 bridges and tunnels, which carry vehicles including automobiles, school buses, motorcycles, and all types of trucks, trailers, and recreational vehicles.
Maritime	Includes a wide range of watercraft and vessels and consists of approximately 95,000 miles of coastline, 361 ports, more than 10,000 miles of navigable waterways, 3.4 million square miles of the Exclusive Economic Zone, and intermodal landside connections, which allow the various modes of transportation to move people and goods to, from, and on the water.

Mass Transit and Passenger Rail	Includes multiple-occupancy vehicles, such as transit buses and facilities, trolleybuses, monorails, heavy (subway) and light rail, passenger rail (including both commuter rail and long-distance rail), automated guide-way transit, inclined planes, and cable cars, designed to transport customers on regional and local routes.
Pipelines	Includes vast networks of pipeline that traverse hundreds of thousands of miles throughout the country, pipeline city gate stations, distribution networks and terminals that transport and distribute nearly all of the Nation's natural gas and about 65 percent of hazardous liquids, as well as various chemicals. These pipeline networks are operated by over 3,000 operators.

Modal protection implementation plans are included as annexes to the SSP. These plans detail the individual characteristics of the mode and explain how each mode will apply risk management approaches to protect its systems, assets, people, and goods. The modal annexes satisfy the requirement to include “the most appropriate, practical, and cost-effective means of defending” the sector against all hazards presenting unacceptable risks.⁴

1.1.1 Sector and Cross-Sector Dependencies

There are many interdependencies among the 18 sectors. Nearly every sector is dependent, to some degree, on the Energy, Communications, Information Technology (IT), and Transportation Systems Sectors. Key dependencies are those that, if interrupted, could significantly impact the performance and overall resilience of the transportation system. Understanding key dependencies enables the sector to identify the potential impacts of, and vulnerabilities to, security threats and natural and manmade disasters.

The following examples highlight some of these critical dependencies:

- The Energy Sector depends on deliveries of coal, crude oil, petroleum products, and natural gas by ship, barge, pipeline, rail, and truck. In return, it produces fuels to power the transportation system.
- The Defense Industrial Base Sector depends on the Nation's air, maritime, rail, and highway networks to move material in support of military operations.
- The Agriculture and Food Sector depends on the security of the transportation portion of the food supply chain to assure safety and security of food shipments.
- The Communications Sector co-locates much of its networking equipment (routers, fiber-optic cable, etc.) along existing transportation routes (rail lines, highway tunnels, and bridges), the destruction of which may impact service availability in wide geographic areas and complicate response efforts in the event of a major incident.
- The transportation network's efficient operations are increasingly dependent upon functions, products, and services provided by Communications Sector and IT Sector entities. Producers and providers of these services, such as the IT and Communications Sectors, have unique roles in cybersecurity, and responsibilities in enhancing the security and resiliency of their cyber infrastructure.
- The Critical Manufacturing, Chemical, and Commercial Facilities Sectors ship goods and services across the entire transportation system utilizing all transportation modes. This is significant to the supply chain as most companies engage in “just in time” reduced inventories rather than stockpiling goods.
- The Emergency Services Sector depends on the resilience of the transportation network to respond effectively to emergencies.

⁴ 49 USC 114 (s)(3)(c).

- The Healthcare and Public Health Sector transports medical supplies through multiple modes of transportation, and relies on special commodities for water treatment and pharmaceuticals, especially in the event of catastrophic emergencies.
- The Postal and Shipping Sector directly depends on transportation, information technology, and communications infrastructure to move packages and mail from origin to destination.
- An incident occurring in the Dams Sector has the potential to directly impact multiple modes of transportation. In addition to maritime traffic disruption, the bridges and tunnels that provide pathways for highway traffic, pipelines, mass transit, railroads, telecommunications, and/or fiber optic cables could also be affected.
- All sectors rely on transportation service for access, supplies, and emergency services.

In addition to cross-sector dependencies, the sector must pay particular attention to interdependencies among the transportation modes. For example, bridges and tunnels provide pathways for pipelines, mass transit, and railroads. A wide range of interconnected cyber assets reinforce, and can complicate, the interdependencies within the sector. Many cyber systems, such as control systems or data centers, are shared between multiple transportation entities. Cyber attacks or other events disrupting these systems could have extended consequences for owners and operators across multiple modes. Furthermore, commodities are shipped through multiple modes which depend on one another for timely and secure deliveries to customers. These modal interdependencies require special consideration of the potential consequences from cascading effects of an incident.

1.1.2 Authorities

The authorities for Federal responsibilities are found in various statutes, directives, and executive orders. These are listed and described in more detail in Appendix 3—Authorities. Some of the sector's most significant protection authorities are derived from the following:

- Aviation and Transportation Security Act of 2001 (ATSA)
- Homeland Security Act of 2002 (HSA)
- Homeland Security Presidential Directive 5, Management of Domestic Incidents (HSPD-5)
- Homeland Security Presidential Directive 7, Critical Infrastructure Identification, Prioritization, and Protection (HSPD-7)
- Homeland Security Presidential Directive 8, National Preparedness (HSPD-8)
- Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53 (9/11 Act)
- Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)
- Maritime Transportation Security Act of 2002 (MTSA)
- Post-Katrina Emergency Management Reform Act of 2006 (Post-Katrina Act)
- Security and Accountability For Every Port Act of 2006 (SAFE Port Act)
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)

1.2 Sector Partners

The term “sector partners” refers to groups and individuals that share in the responsibility for protecting the sector's assets, systems, and networks. These include Federal, State, local, tribal, territorial, and foreign governmental entities, owners and operators, and representative organizations, regional organizations and coalitions, academic and professional entities, international organizations, non-profit employee representative organizations, and volunteer organizations. The sector engages its partners through a collaborative process to determine sector goals, priorities, and risk methodologies as they relate to the

sector's physical, human, and cyber elements of critical infrastructure. The modal annexes provide more detailed descriptions of the sector's partnerships.

1.2.1 Sector-Specific Agencies

Under the requirements of HSPD-7, the Department of Homeland Security (DHS) delegated SSA responsibilities for the sector to TSA and for the maritime mode to the USCG. SSA responsibilities include engaging partners in cooperative processes to:

- Identify key assets;
- Determine risks;
- Prioritize protection objectives;
- Develop risk reduction programs and resiliency strategies;
- Implement risk reduction programs and resiliency strategies; and
- Measure progress toward reducing risks.

Transportation Security Administration. TSA has a lead role for security of the aviation and surface transportation modes and supports the USCG as the lead for maritime security. As part of its security mission, TSA is responsible for assessing intelligence, issuing and enforcing security directives (including no-notice emergency regulations), ensuring the adequacy of security measures at transportation facilities, and assuring effective and timely distribution of intelligence to sector partners. TSA collaborates with DOT—in its capacity as the lead for transportation safety, response, and recovery—to manage protection and resiliency programs for all hazards.

United States Coast Guard. The USCG is a multi-mission maritime service and one of the Nation's five Armed Services. Its mission is to protect the public, the environment, and U.S. economic interests in the Nation's ports, on navigable waterways inland, along the coast, on the high seas, or in any maritime region, as required to support national security. In the event of a maritime incident, the USCG will often act in a first-responder capacity. The USCG has the primary responsibility for the security of the maritime domain, including coordinating mitigation measures to expedite the recovery of maritime infrastructure and transportation systems and to support incident response in coordination with the Department of Defense (DoD).

Appendix 4—Transportation Systems Sector Partners provides an overview of other Federal transportation partners, in addition to advisory councils, academia, research centers, and think tanks, all supporting the sector in achieving its goals.

The SSAs provide a Sector Annual Report (SAR) to DHS on the progress of implementing the goals of the SSP. The SSAs also participate in programs to collect and disseminate intelligence and infrastructure information, to identify critical infrastructure and foreign dependencies, to improve protection and resiliency awareness, and to support Federal response and recovery priorities during disasters.

1.2.2 The Sector Partnership Model

The NIPP Sector Partnership Model provides a mechanism for engagement with private and public sector partners to reduce security risks. The Transportation Systems Sector Partnership Model (SPM) conforms to the NIPP model and augments it with Federal advisory committees and other regional and modal forums as explained in the modal annexes.

Under the SPM, the sector-level Government Coordinating Council (GCC) and Sector Coordinating Council (SCC) provide strategic direction for sector protection and resiliency initiatives and risk management processes. The sector-level SCC had not formed at the time of this writing; however, it is expected to become a key part of the SPM. Its formation is a short-term sector objective. It is anticipated that the sector-level GCC and SCC will meet jointly to exchange views on strategic priorities and other matters essential for achieving the risk-reduction objectives in the SSP.

The functions of the SPM fall under the aegis of the Critical Infrastructure Partnership Advisory Council (CIPAC) for modal GCCs and SCCs. The SPM conforms to the Federal Advisory Committee Act (FACA)⁵ governing the establishment, operations, oversight, and termination of advisory bodies to assure their objectivity and access to the public. The GCCs and SCCs are chartered under the rules governing CIPAC working groups. This provides the legal construct for collaborative engagement with stakeholders as required by law and presidential directives.

Government Coordinating Councils

Figure 1-1: Transportation Systems Sector GCC Organization

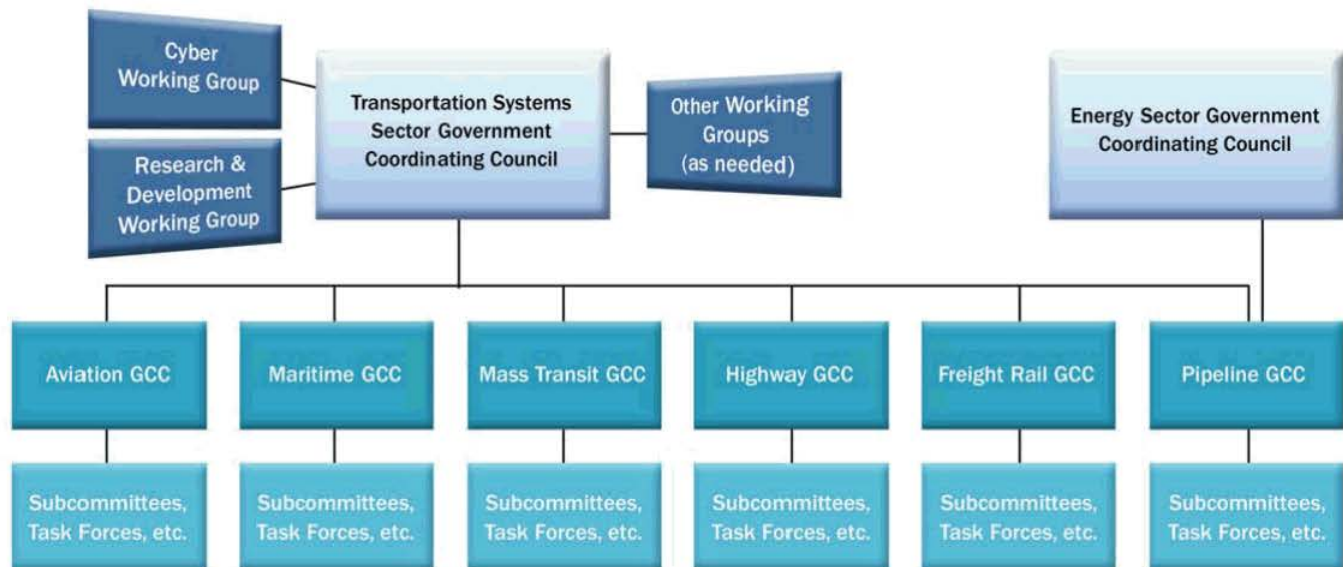


Figure 1-1 depicts the GCC organizational framework, including the relationship between the sector and modal level GCCs. The primary missions of the GCCs are to coordinate the development of transportation infrastructure protection and resiliency strategies and activities, to assure collaboration with sector partners, and to monitor the effectiveness of risk management programs. The GCCs may identify gaps in plans, programs, policies, procedures, and strategies, and serve as the forum to work with the private sector to develop security and resiliency objectives, policies, standards, and plans. TSA and DHS Office of Infrastructure Protection (IP) co-chair the Sector GCC.

The Transportation Systems Sector GCC includes representatives from the following departments and agencies (further described in Appendix 4—Transportation Systems Sector Partners):

- Department of Homeland Security
 - TSA
 - USCG
 - IP
- Department of Transportation
- Department of State (DOS)

⁵ Public Law 92-463.

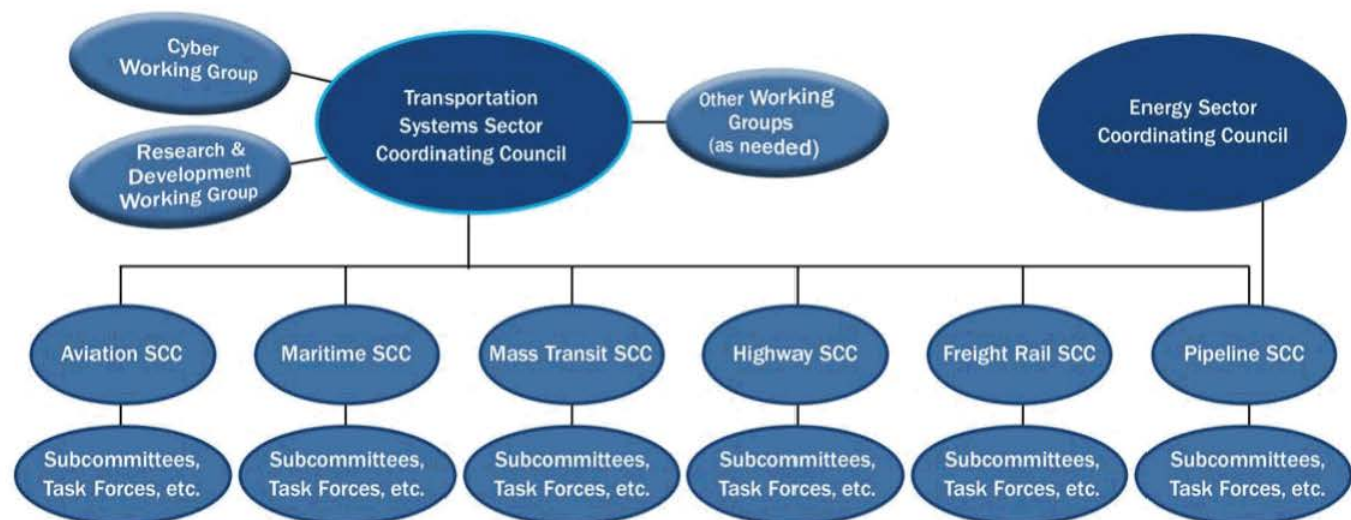
- Department of Commerce (DOC)
- Department of Energy (DOE)
- Department of Defense
- State, local, tribal, and territorial representatives

TSA representatives from each mode within the sector chair the modal GCCs (with the exception of the Maritime GCC, which the USCG chairs). The modal GCCs' members and/or agencies are identified in the modal annexes.

In figures 1-1 and 1-2, the blocks referring to “Other Working Groups” recognize that working groups may be created and developed as deemed necessary within the GCCs or jointly with the SCCs for specific functions. For example, the joint Transportation Systems Sector Cyber Working Group (TSS CWG) is composed of government and private sector specialists whose task is to develop a strategy to guide the sector’s and the modes’ efforts to identify and reduce cyber risks. Working groups may be chartered to address such issues as risk management, resiliency, information sharing, program measurement, or other special needs. The working groups provide GCC members with findings, recommendations, advice, or specific deliverables, as indicated in their charters.

Sector Coordinating Councils

Figure 1-2: Transportation Systems SCC Organization



Private sector partners contribute to security policies and plans through the Transportation Systems SCC framework. Figure 1-2 depicts the organizational framework of the SCCs. The framework mirrors that of the GCC, thus facilitating communications and development of working groups to address sector and modal issues. Each modal SCC chartered under CIPAC forms voluntarily. SCC membership for the modes is fully described in the modal annexes and typically includes representatives of sector owners, operators, and members of related trade associations. In modes where the SCCs are not functional, other mechanisms, such as advisory councils, are venues for partners to effectively address modal issues. The sector-level SCC, when formed and certified under CIPAC, will include representation from a wide range of transportation service providers, cargo carriers, and freight forwarders.

The SCC function serves an important role in providing expertise and leadership in sector protection activities including, but not limited to:

- Contributing to an effective risk management approach by working in partnership with the GCCs to identify and provide information regarding security and resiliency priorities and activities within the sector;
- Planning response and recovery activities by participating in information sharing and other communications during and after an incident or events such as pandemic influenza, natural disasters, or terrorists attacks;
- Sharing information related to best practices, credible threats, risk data, incidents, domain awareness campaigns, and others, with sector partners;
- Identifying and implementing the information-sharing mechanisms that are most appropriate for their respective modes;
- Supporting the GCCs to enhance existing working groups and, establishing additional working groups, as needed; and
- Providing industry linkage to the National Infrastructure Coordinating Center (NICC), a 24/7 operations center that maintains ongoing operational and situational awareness of the Nation's CIKR sectors.

1.2.3 Other Federal Departments and Agencies

This section provides a brief description of other Federal agencies with transportation security-related missions. Appendix 4—Transportation Systems Sector Partners includes a comprehensive list of other Federal partners, as well as advisory councils, academia, research centers, and think tanks that work collaboratively with the Transportation Systems GCCs and SCCs to achieve the sector's mission and goals.

Customs and Border Protection. CBP is a DHS agency that protects America at its borders and ports of entry from the introduction of dangerous people and goods into the United States. CBP accomplishes this wide-ranging responsibility through a risk-based, layered enforcement strategy using advanced technologies, information analysis, and partnership programs.

Department of Commerce. DOC promotes economic development and international trade and protects national security through export controls for technologies and weapons. DOC's transportation security equities relate primarily to supply chain services of the transportation industry. DOC's National Institute of Standards and Technology (NIST) provides non-regulatory standards to enhance U.S. industrial product quality, competitiveness, and security. The National Oceanic and Atmospheric Administration (NOAA) provides daily weather forecasts, severe storm warnings, and climate monitoring to fisheries management, coastal restoration, and marine commerce.

Department of Defense. DoD is responsible for defending the Nation from external threats and owns a wide spectrum of support resources that could be requested during a natural or man-made disaster involving transportation-related assets. DoD has significant private sector transportation security equities, since it places vast requirements on commercial transportation providers to move passengers and freight worldwide. DoD, as a member of the Transportation Systems Sector GCC, contributes to transportation security policies and decisions. Specific DoD agencies with transportation security responsibilities are described in appendix 4.

Department of Energy. The Energy and Transportation Systems Sectors have a number of cross-sector dependencies. As the SSA for the Energy Sector, DOE is responsible for ensuring the security of the Nation's electricity, petroleum, and natural gas energy resources. The sector's reliance on hazardous liquid and natural gas pipelines highlights the interdependency with the Transportation Sector. Consequently, DOE and TSA have established a cross-sector partnership to coordinate security programs in the oil and natural gas industries.

Department of Justice. DOJ's mission is to enforce the law and defend the interests of the United States according to the law; to ensure public safety against threats foreign and domestic; to provide Federal leadership in preventing and controlling crime; to seek just punishment for those guilty of unlawful behavior; and to ensure fair and impartial administration of justice for all Americans. DOJ acts to reduce criminal and terrorists threats, and investigates and prosecutes actual or attempted attacks on, sabotage of, or disruptions of critical infrastructure in collaboration with DHS. As part of the national effort to identify,

prevent, and prosecute terrorists, TSA will work closely with the Federal Bureau of Investigation (FBI), which maintains the lead responsibility for investigations of terrorists' acts or threats by individuals or groups inside the United States.

Department of Transportation. DOT has the responsibility for ensuring a safe, efficient, and accessible transportation system that meets national interests and enhances the quality of life of the American people. It meets these challenges through grants, regulation, enforcement, research and development, and other means. DOT modal administrations manage many transportation programs that directly affect the protection and resilience of critical transportation infrastructure. As directed in HSPD-7 and various statutes, DOT and DHS collaborate on matters related to transportation security and infrastructure protection. Under the National Response Framework (NRF), DOT is the lead agency for coordinating Federal transportation activities during emergencies and for response and recovery operations.

Department of State. DOS conducts diplomacy, a mission based on the role of the Secretary of State as the President's principal foreign policy advisor. DOS leads representation of the United States overseas and advocates U.S. policies with foreign governments and international organizations. DOS plays an important role in coordinating transportation protection issues with foreign governments. DOS addresses issues concerning the protection and security of pipelines that cross national boundaries, transportation-related concerns over international waterways, and the transportation of goods and people across international boundaries by the aviation mode.

1.2.4 State, Local, Tribal, and Territorial Governments

State, local, tribal, and territorial governments manage sector protection efforts within their respective jurisdictions. The State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC), established in 2007, represents these sector partners within the NIPP partnership framework.

State governments serve as crucial coordination hubs among local jurisdictions, across sectors, and between regional entities. They bring together the authorities, capacities, and resources necessary for prevention, protection, response, and recovery. State and local agencies are often first on the scene of a transportation security incident, natural or manmade. Local governments represent the "front lines" for first responses to incidents involving sector assets. In accordance with the NRF, Federal agencies provide support to the State and local authorities to meet emergency response needs and to coordinate the resources necessary for recovery.

In order to meet resiliency objectives, State, local, tribal, and territorial authorities also assist DHS, DOT, and the sector in collecting information about critical transportation infrastructure prior to an event and in providing impact assessments as incidents develop and stabilize.

1.2.5 Regional Coalitions

Regional coalitions play an important role in protection and resiliency planning and programming. For example, the maritime mode includes regional port complexes and the mass transit and passenger rail mode includes regional transit systems. Transportation Security Inspectors are assigned to cover the key rail and mass transit facilities in metropolitan regions around the country. In addition to other duties, inspectors serve as the SSA's liaison to regional mass transit agencies and to their Federal, State, and local sector partners.

Regional coalitions in large metropolitan areas, known as metropolitan planning organizations (MPOs), have responsibility for planning, programming, and coordinating Federal highway and transit investments. These metropolitan areas are vital to the Nation's economic well-being due to the density of industries and businesses and the large number of citizens living and working within and around them. Transportation services are a vital component of the economic vitality of these areas. The MPOs coordinate partnerships at the State and local levels to enhance the safe and secure transportation of goods and people. Furthermore, MPOs assist metropolitan areas in planning for evacuations of areas impacted in a catastrophic event.

1.2.6 International Organizations and Foreign Governments

In a single calendar month, the import and export of goods and services to and from the United States exceeds 287 billion dollars.⁶ As the data indicates, large volumes of merchandise enter the United States daily via the global supply chain, through various types of transportation such as container ships, trucks, rail cars, and airplanes from across the oceans, and from our border countries, Canada and Mexico.

The sector recognizes the importance of international partnerships, and the continuous need for international engagement to further U.S. objectives and interests. Specifically, the sector works with international partners to:

- Use existing mechanisms to exchange and share effective practices to further Transportation Systems Sector goals and objectives;
- Develop new mechanisms, where appropriate, to promote critical infrastructure protection and identify critical foreign dependencies;
- Continue to identify and understand threats, assess vulnerabilities, and determine potential impacts of incidents to the global transportation system and supply chain;
- Promote measures that safeguard the movement of people, goods, and services through international transportation systems; and
- Strengthen transportation preparedness and resiliency across all modes of the global transportation network.

Strengthening transportation preparedness and resiliency across all modes of the global transportation network requires strong collaboration worldwide to protect the traveling public from all hazards and reduces the potential for a disruption in the flow of commerce. The overarching goal is to strengthen transportation security practices by building and expanding partnerships with groups such as: the European Union (EU); the Group of Eight members (G8)—the United States, Canada, France, Germany, Italy, Japan, Russia, and the United Kingdom; the Asia-Pacific Economic Cooperation Forum; the International Civil Aviation Organization; the International Maritime Organization; and the Organization of American States. Comprehensive guidance on international partnerships can be found in the NIPP in section 4.1.4 and appendix 1B.

In addition to strengthening partnerships with established groups, the sector engages through bilateral and multilateral partnerships with key international partners. These bilateral working groups provide the sector with the opportunity to exchange information and engage in cooperative activities on existing and possible future protection and security measures for all modes of transportation.

1.2.7 Private and Public Owners and Operators

A collaborative partnership between sector government partners and owners and operators is essential to improve the preparedness of, and reduce the risks to, transportation assets, systems, and networks for all hazards. Owners and operators participate voluntarily in a variety of ways to protect the sector's infrastructure and to assure its resiliency through business continuity planning and risk mitigation activities. In the wake of the attacks of September 11, 2001, many trade associations developed and encouraged participation in security best practices, planning, training, and exercises. Numerous owners and operators of transportation infrastructure as well as members of representative associations provide technical expertise during the development of voluntary standards and regulations. This expertise expands across human, physical, and cyber elements of the sector's critical infrastructure. For example, the sector relies on its owners and operators to identify critical cyber components of their operations and to assist in determining strategies for evaluating cyber risks and selecting countermeasures to reduce those risks.

⁶ U.S. International Trade in Goods and Services, August 2009. U.S. Census Bureau, U.S. Bureau of Economic Analysis, U.S. Department of Commerce, U.S., released October 9, 2009.

1.3 Sector Goals and Objectives

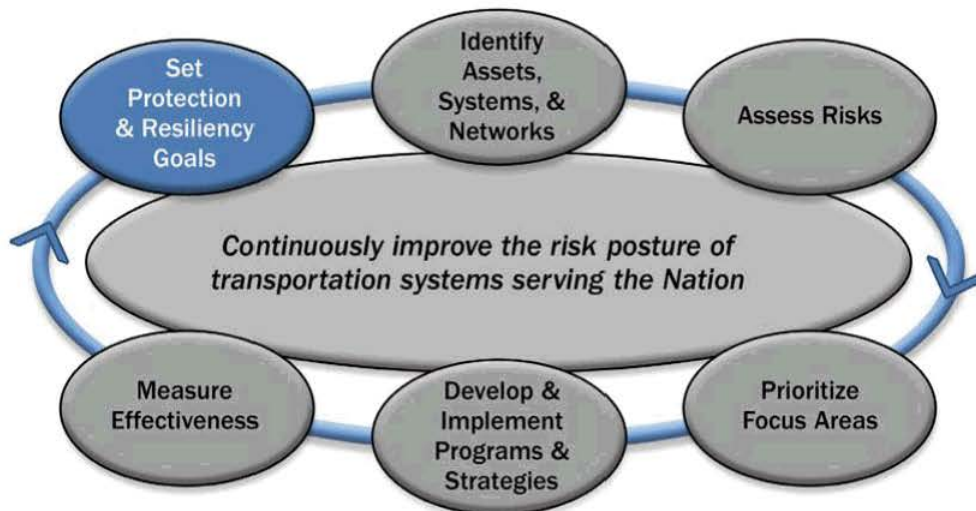
The sector's goals and objectives provided below are consistent with the goals outlined in the President's homeland security agenda, sector priorities, and the statutory imperatives for protecting the transportation system and improving resiliency of its critical infrastructure and networks. The President's Guiding Principles for Homeland Security,⁷ released in 2009, are stated as follows:

The President's Guiding Principles for Homeland Security

Ensuring the resilience of our critical infrastructure is vital to homeland security. Working with the private sector and government partners at all levels, we will develop an effective, holistic, critical infrastructure protection and resiliency plan that centers on investments in business, technology, civil society, government, and education. We will invest in our Nation's most pressing short- and long-term infrastructure needs, including modernizing our electrical grid; upgrading our highway, rail, maritime, and aviation infrastructure; enhancing security within our chemical and nuclear sectors; and safeguarding the public transportation systems that Americans use every day.

These goals and objectives shape the sector partners' approach for managing sector risk. The risk management framework depicted in figure 1-3 is described in chapters 2 through 6. The framework is based on the 2009 NIPP risk management criteria, and provides overarching guidelines for risk management within the sector. The different stages of the framework directly support fulfilling the sector's mission, described below.

Figure 1-3: Transportation Systems Sector Risk Management Framework



⁷ http://www.whitehouse.gov/issues/homeland_security.

The sector's vision, mission, goals, and objectives are as follows:

Vision

A secure and resilient transportation system, enabling legitimate travelers and goods to move without significant disruption of commerce, undue fear of harm, or loss of civil liberties.

Mission

Continuously improve the risk posture of transportation systems serving the Nation.

Goal 1: Prevent and deter acts of terrorism using, or against, the transportation system.

Objectives

- Implement flexible, layered, and measurably effective security programs using risk management principles.
- Increase vigilance of travelers and transportation workers. The traveling public and transportation workers can serve as force multipliers to Federal, State, and local law enforcement efforts.
- Minimize the impact of security policies and programs to promote the freedom of movement of goods and people.

Goal 2: Enhance the all-hazard preparedness and resilience of the global transportation system to safeguard U.S. national interests.

Objectives

- Continually identify and assess critical sector infrastructure using the risk management framework.
- Analyze infrastructure assessments and focus efforts to mitigate risks, to improve overall network survivability from all hazards, and to maintain continuity of operations during an incident.
- Work to develop and enhance preparedness and resilience activities that include first-responder actions and the plans, training, and exercises that support all sector partners.
- Identify capacity or technology gaps in response capabilities necessary for the expeditious recovery of critical systems.
- Develop sector processes to determine critical cyber assets, systems, and networks and identify and implement measures to address strategic cybersecurity priorities.

Goal 3: Improve the effective use of resources for transportation security.

Objectives

- Align sector resources with the highest priority protection and resiliency needs including risk and economic analyses as decision criteria.
- Enhance effective use of resources by minimizing unnecessary duplication of efforts, improving coordination, and aligning resources to address the highest risks of the sector.

- Promote sector participation in the development and implementation of public sector programs for asset, system, and network protection.
- Ensure coordination and enhance risk-based prioritization of sector security research, development, test, and evaluation (RDT&E) efforts.
- Coordinate policy and minimize duplication of efforts by Federal, State, and local government agencies to improve the safety and security of the sector.

Goal 4: Improve sector situational awareness, understanding, and collaboration.

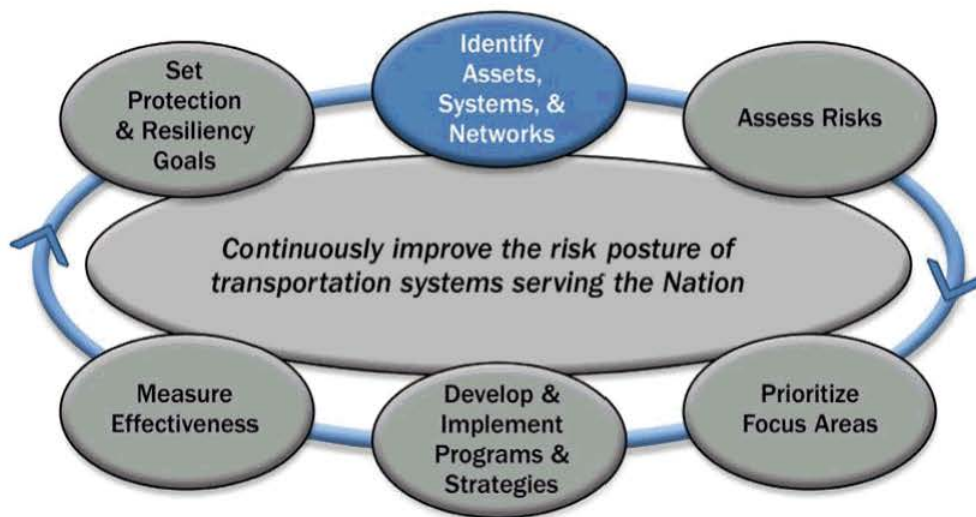
Objectives

- Strengthen partnerships to further national interests. Develop enhanced security awareness and coordination as a force multiplier.
- Continuously assess threats and enhance timely information-sharing among sector partners.
- Advance preparedness and resiliency concepts and risk management best practices within the sector.
- Understand intermodal and cross-sector intra-dependencies, and collaborate with partners to enhance knowledge.

1.4 Value Proposition

The SSP is valuable to the American people if it enables the responsible public and private officials—the sector’s partners—to implement programs and activities that create a secure and resilient transportation network as described in the sector’s vision statement. In collaboration with the sector’s partners, the SSP should be the commonly shared blueprint for building an all-hazards preparedness, protection, and resiliency framework. In addition, the SSP consolidates and combines several strategies and national plans to provide a single comprehensive plan for the sector. The jointly developed risk management process provides a means for all of the sector’s partners to have a voice in security, infrastructure protection, and resiliency policy development.

2. Identify Assets, Systems, and Networks



This chapter describes the processes for identifying the sector's critical infrastructure. Critical infrastructure includes those assets, systems, and networks, which if damaged, could result in significant consequences—impacts on national economic security, national public health and safety, public confidence, loss of life, or some combination of these.

Determining the criticality of transportation infrastructure is a key step in the larger risk management process aimed at identifying critical infrastructure vulnerabilities, applying appropriate countermeasures, and measuring risk reduction. The identification of critical infrastructure also assists Federal, State, local, tribal, and territorial authorities as well as the private sector in incident response and recovery planning—important aspects of system resiliency. Furthermore, understanding the relationships between individual assets, systems, and networks is vital to evaluating the criticality of physical and virtual systems and networks.

2.1 Defining Information Parameters

Information on sector infrastructure assists in risk management and incident response, and data parameters are designed around these two objectives. The parameters for risk management data, at the modal and strategic level, address the consequences of, and the vulnerabilities to, specific threats. Incident management data parameters are oriented to infrastructure type, location, and ownership. Information requirements associated with risk management of natural disasters, pandemics and public health emergencies, and high-consequence accidents are different from those required for security threats. The sector

will continue to expand its understanding of the data requirements and sources for risk management of terrorism and all-hazards events.

In conjunction with DHS, the sector established an infrastructure taxonomy as a common lexicon of various groups, sub-groups, and types of assets in each mode. For example, airports are a group of like assets in the aviation mode. Within airports there are certified airports, non-certified airports, military airports, and private airports. Within certified airports there are Category X and Categories I through IV. Similar categorizations and subdivisions occur in all of the transportation modes. The complete taxonomy listing of sector assets is provided in Appendix 6—Taxonomy.

Data collected for risk management supports the assessment of criticality based on potential consequences of the loss or incapacitation of the infrastructure. Consequence data includes the estimated costs of repair or replacement of the infrastructure, emergency response, economic impacts, potential injuries or loss of life, and psychological impacts. Since redundancies and effective countermeasures reduce the potential consequences, information on countermeasure effectiveness is also sought.

Vulnerability data is collected for the physical, human, and cyber elements of infrastructure. Physical vulnerability data might include perimeter security, access controls, surveillance, screening and sensors, visible deterrent operations, and resilient structures. Human vulnerabilities are addressed by security threat assessments of employees, credentialing, detection of threatening insider behaviors, training and awareness, and information sharing processes. Cyber vulnerabilities can have physical, human, technology, and software dimensions. For example, sensitive information on storage media must be protected against unauthorized access and theft, and intrusion protections must be installed in network terminals and computers.

Infrastructure Data Warehouse

DHS uses infrastructure information to manage Federal infrastructure protection and resiliency programs, to inform Federal emergency responses, and to determine regional priorities for recovery efforts. Infrastructure data is retained in the DHS Infrastructure Data Warehouse (IDW). The SSAs, Federal and State partners, and the sector's owners and operators contribute to the collection of data through data calls, site visits, security audits, or compliance inspections. Information voluntarily submitted may be protected from disclosure or from use for litigation or regulation development at the owner's or operator's request under rules for the legislatively directed Protection of Critical Infrastructure Information (PCII) program.

2.2 Collecting Infrastructure Information

The collection of infrastructure information is a shared responsibility. The SSAs, DHS, DOT, DOE, other Federal and industry partners and owners and operators contribute information through a number of venues. The SSAs and DHS conduct site visits, compliance inspections, and audits of assets and systems. Owners and operators support these visits by providing the requested physical, human, and cyber information voluntarily or as required by regulations. The information collected during these visits is deposited in the IDW and in TSA's modal databases. TSA is developing the parameters for a repository of risk management information to centralize data storage.

Annually, DHS conducts the National Critical Infrastructure Prioritization Program (NCIPP), formerly known as the Tier I/Tier II Process. IP develops consequence-based criteria for identifying infrastructure whose disruption could cause nationally or regionally catastrophic effects (i.e., is nationally critical). The States, Territories, and the SSAs then submit nominations to DHS for inclusion on this "nationally critical" list. DHS adjudicates the nominations—in consultation with subject matter experts from the SSAs—and merges them with submissions from other sectors to compile a single list of nationally critical infrastructure.

Safety and security visits by multiple Federal and State agencies can potentially create an undue burden on owners and operators. The sector will enhance the coordination of visits and data collection efforts to minimize impacts on the industry as well as to assure that a common set of data is used for risk management, protection, and resiliency purposes across agencies.

2.3 Verifying and Updating Infrastructure Information

The NCIPP provides an opportunity for the sector to reconsider information previously submitted, for accuracy and for changes in risks. Under Federal law, infrastructure information collected by DHS during site visits is protected at the request of the asset owner or operator from use for regulatory purposes, Freedom of Information Act requests, State and local disclosure laws, and use in civil litigation. Consequently, infrastructure information in the IDW is not available to SSAs having regulatory authority.

2.4 Critical Cyber Infrastructure Identification

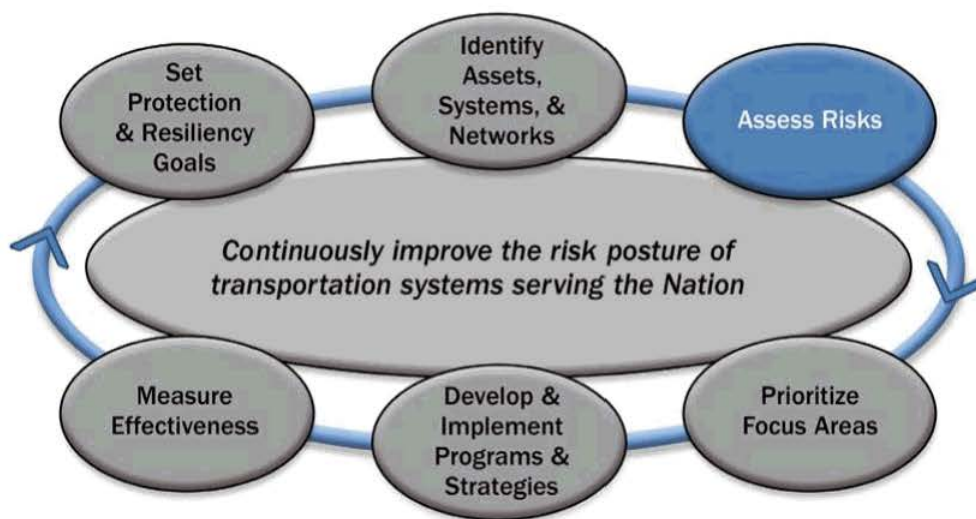
The sector defines critical cyber infrastructure as those cyber systems and assets that if incapacitated or disrupted could cause significant harm to transportation systems, or have a debilitating impact on the national security, the economy, public health or safety, or the environment.

The sector's process for identifying critical cyber infrastructure is founded on each mode's evaluation of its critical assets and systems. Due to the vital function of cyber infrastructure in transportation operations, modal experts will determine the criticality of cyber systems. The TSS CWG contributes intermodal and cross-sector cyber expertise from the public and private sectors to facilitate determinations of criticality and to assure consistency across the modes for evaluating cyber assets and systems including cyber dependencies and interdependencies.

Federal policy guiding the identification of critical cyber infrastructure is evolving through collaborative forums led by the National Security Council and Federal departments, such as the Quadrennial Homeland Security Review. Furthermore, it is expected that as critical cyber infrastructure lists are developed, they will be incorporated, as appropriate, into the NCIPP.



3. Assess Risks



This chapter addresses the assessment phase of the risk management framework. The size, complexity, and openness of the sector as well as the dynamic nature of the security threats create challenges for assessing risks, including:

- Uncertainty as to the types of threats to the transportation system;
- Difficulties of predicting the likelihood and consequences of known risks;
- Inestimable nature of unknown risks;
- Wide spectrum of risks, often requiring different assessment methodologies;
- Unique differences between risk assessments for manmade incidents (including terrorism) versus natural disasters;
- Creative and adaptive nature of terrorists; and
- Widely varying preparedness and response capabilities and countermeasures within the groups and subgroups of modal infrastructure.

These challenges preclude any single assessment methodology. Consequently, the sector's risk assessment framework establishes a process and general principles to guide risk assessments conducted to inform sector decisionmaking. The process and principles apply to strategic or cross-modal assessments and to tactical assessments within a mode, sub-modal group, or system. The risk management framework will be applied to the physical, human, and cyber components of infrastructure.

Risk assessments of natural disasters focus on the likelihood of the disaster and the anticipated consequences. For example, regional risks for hurricanes or tornados could be determined from statistical records to determine event probabilities and estimates of consequences. These assessments may be relatively straightforward using the basic risk equation:

$$\text{Risk} = f(\text{Probability, Consequence})$$

Since terrorist risks are not probabilistic, the following equation developed by the Government Accountability Office in 2001, has been widely adopted for calculating terrorism-related risks:

$$\text{Risk} = f(\text{Threat, Vulnerability, Consequence})$$

Threat, vulnerability, and consequence are defined as:

- Threat: An individual, entity, or action that has the potential to deliberately harm life and/or property;
- Vulnerability: Physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard; and
- Consequence: The effect of an event, incident, or occurrence.

3.1 Use of Risk Assessment in the Sector

Risk assessments of the transportation system examine the probability and the consequences of an undesirable event affecting, or resulting from, sector assets, systems, or networks. As a result, transportation system risk is characterized in two fundamental and non-mutually exclusive ways, as referenced in Goal 1:

- (1) Risk to the Transportation System
- (2) Risk from the Transportation System

The sector's members use risk assessments for a number of purposes including establishing strategic priorities, informing countermeasure selection, developing risk reduction measures, and determining budget and resource allocation priorities. In all cases, the risk assessments are just one of multiple factors to be considered in risk management decisions.

3.2 Assessing Sector Assets, Systems, and Networks

Risk assessments are intended to inform the sector's decisionmakers regarding priorities, programs, and budgets for reducing risks to infrastructure from all hazards. While there is scant historic data for terrorist attacks in the United States, some terror threats are clearly known and understood based on criminal investigations, intelligence analyses of intents and capabilities, and past attacks. Other threats, particularly those stemming from the use of novel attack vectors or executed by lone individuals, are beyond our ability to assess. Intelligence assessments and terrorist role-playing provide important insights regarding emerging or potential threats, but the margins of error may be considerable and some threats may not be anticipated. Decisionmakers must be prepared to use emerging intelligence assessments as an essential aspect of their risk management approach to enable

the expeditious adjustment of security priorities and resources. Recognizing the varied and dynamic contexts of risk management decisions, the sector's risk management approach is designed to assist decisionmakers in mitigating known threats and narrowing the creative options for unknown threats.

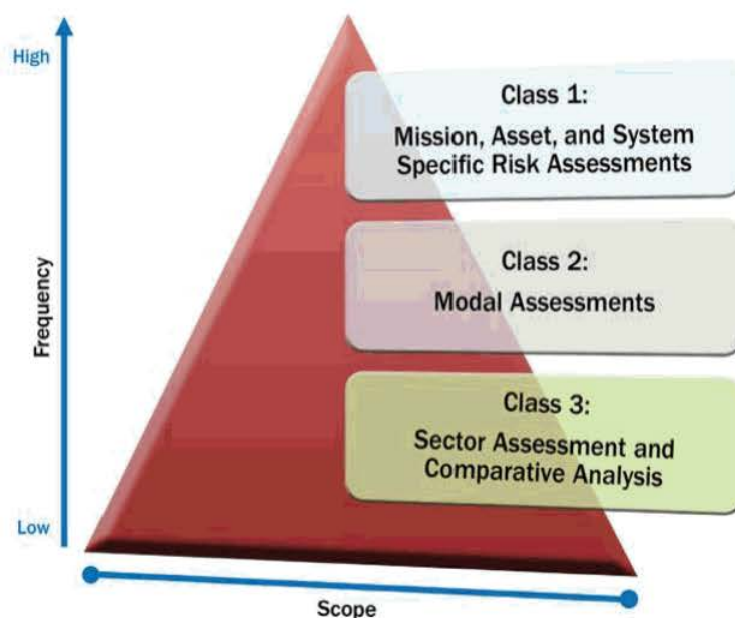
Assessments of transportation assets and systems consider information such as cargo or passenger volume, proximity to population centers, and system dependence on a particular asset. In refining the identification of transportation infrastructure assets, more detailed assessments may be useful to change or add to the initially identified assets and systems. To the extent practical, the sector applies the following risk management principles:⁸

- **Practicality.** The practicality principle suggests that the assessment methodology be developed in full awareness of the limitations of available data on threats, vulnerabilities, and consequences. The assessment methodology chosen must be practical for the available data and decision requirements to be served. The methodology selected should also conform to resource, time, and budgetary constraints.
- **Appropriateness.** Risk assessments and analyses should be appropriate for the purpose of the assessment. Assessments for determining strategic priorities differ in scope and methodology from those used to determine asset risks for a specific threat. Assessments for identifying vulnerabilities and applying countermeasures differ from those for deploying resources during an incident.
- **Comparability.** Risk assessment tools should allow for comparisons of the risks among different threat scenarios or among different infrastructure categories being considered. Since risk assessments are used to inform decisions about risk reduction priorities, ideally the methodologies should produce comparable results.
- **Transparency.** To effectively inform decisionmaking, risk management information must have a degree of transparency during assessment, analysis, and development of alternative strategies. The transparency principle assures the openness to scrutiny of the methodology and the data.
- **Documentation.** Risk assessments intended for sector consideration should be documented sufficiently to establish a record of the methodology, assumptions, data sources, data limitations, data, and conclusions. The documentation should be such that the assessment could be repeated with similar results. Proper documentation enables critical analyses of the approach and results and the development of metrics to assist in determining risk reduction.
- **Partnership.** While assessments may be undertaken independently by infrastructure owners and operators or by government agencies, many are conducted jointly. As the sector's risk management framework envisions collaborative processes to reduce priority risks, joint participation in the assessment process promotes shared confidence in the results, and a common understanding of the vulnerabilities that must be mitigated.

The ability to conduct defensible risk assessments is directly related to the availability and accuracy of information on threats, consequences, and infrastructure vulnerabilities. The sector continues to build an infrastructure database for assessments, program decisions, and risk reduction measures of owners and operators. As transportation system intelligence and information is gathered it is used in three classes of risk assessments, as depicted in figure 3-1. These assessments may vary in methodology depending on their scope and purpose, and can be broadly characterized as Mission, Asset, and System Specific Risk Assessments (MASSRA), modal risk assessments, and sector cross-modal risk assessments.

⁸ These principles build on the broader set of risk management principles established by the Office of Management and Budget (OMB) in 1995 to define risk analysis and its purposes, and to generally guide agencies as they use risk analysis in the regulatory context. The DHS RMA Integrated Risk Management Framework risk management principles succinctly describe important characteristics of homeland security risk management that are wholly consistent with the overall principles established by OMB while specifically focusing on the key principles for risk management by DHS. See U.S. Office of Mgmt. and Budget, Memorandum for the Regulatory Working Group, Principles for Risk Analysis (1995), at www.whitehouse.gov/omb/inforeg/regpol/jan1995_risk_analysis_principles.pdf.

Figure 3-1: Three Classes of Risk Assessments



Class 1: Mission, Asset, and System Specific Risk Assessments

MASSRA focus on one or more of the risk elements or on scenario-specific assessments (for example, a blast effect analysis on a certain type of conveyance). Physical security self-assessments conducted by transportation service providers that estimate vulnerability⁹ also fall into the MASSRA category. These assessments generally do not cross jurisdictional lines and have a narrow, specific focus. They generally provide a detailed analysis of infrastructure vulnerabilities and can be used to determine which countermeasures should be used to mitigate risk. MASSRA are commonly referred to as field assessments in a Federal context as they are often conducted by local experts who use a centralized methodology. Assessments conducted by owners and operators of cyber systems within the operation of a company also fall within the MASSRA class.

Class 2: Modal Risk Assessments

Modal risk assessments are used to identify how best to determine or validate high-risk focus areas within a mode of transportation. These assessments also help to establish the sector's priorities for a specific mode. As with all risk assessment classes, Class 2 assessments vary with respect to the type of risks and hazard categories being assessed across physical, human, and cyber elements. For example, the SSAs conduct modal threat assessments annually in partnership with the Office of Naval Intelligence, DOT, and other members of the Intelligence Community (IC).

TSA's Transportation Sector Security Risk Assessment (TSSRA) tool is used to conduct modal security risk assessments for each of the primary transportation modes, as well as sub-modal groups, such as the school bus transportation system. As SSA for the maritime mode, the USCG uses the Maritime Security Risk Analysis Model (MSRAM) and other inputs to provide the mari-

⁹ An assessment of Criticality, Accessibility, Recoverability, Vulnerability, Effect, and Recognizability (CARVER) was originally an offensive target assessment tool developed for use by DoD to evaluate the value of enemy targets and determining how best to exploit identified vulnerabilities. The same methodology was later adopted for DoD Force Protection and is now the basis for many vulnerability assessment methodologies used to evaluate CIKR. USCG guidance for MTSA required self-security assessments of vessels and port facilities to follow a CARVER-like approach.

time risk information to TSSRA. FEMA, DOT, and other organizations may conduct similar assessments or case studies of the potential consequences of natural disasters that would fit within Class 2 assessments.

Class 3: Cross-Modal Comparative Analysis

Class 3 assessments are cross-modal risk assessments focusing on two or more modes, or on the entire sector. TSSRA, previously described as a modal risk assessment method, is also an example of a cross-modal comparative analysis method. These analyses help identify strategic planning priorities and define long-term visions. Cross-modal analyses inform key leadership decisions, including investments in countermeasures. For example, a sector-wide security assessment could identify an improvised explosive device (IED) attack to underwater tunnels as a top threat. At the same time, safety and emergency management assessments may identify the same tunnels as being in need of repair. In such cases, sector leaders should maximize the effectiveness of resources by seeking options to enhance resilience, improve safety, and reduce security risks.

Conclusions drawn from cross-modal analysis should work to ensure that they reduce risk rather than shift it from one mode to another.

Risk Assessment Classes: Summary

These three risk assessment types may be conducted concurrently and/or independently by various sector partners. Once the assessments take place and the results are analyzed and disseminated, they are sent to the sector's leadership as tools to aid in decisionmaking processes. These assessments are considered along with other factors, such as cross sector impacts, mandates, and constraints, when determining the sector's risk priorities as described in chapter 4. Conclusions drawn from cross-modal analyses should work to ensure that they reduce risk rather than shift it from one mode to another.

3.2.1 Featured Risk Assessment Methods

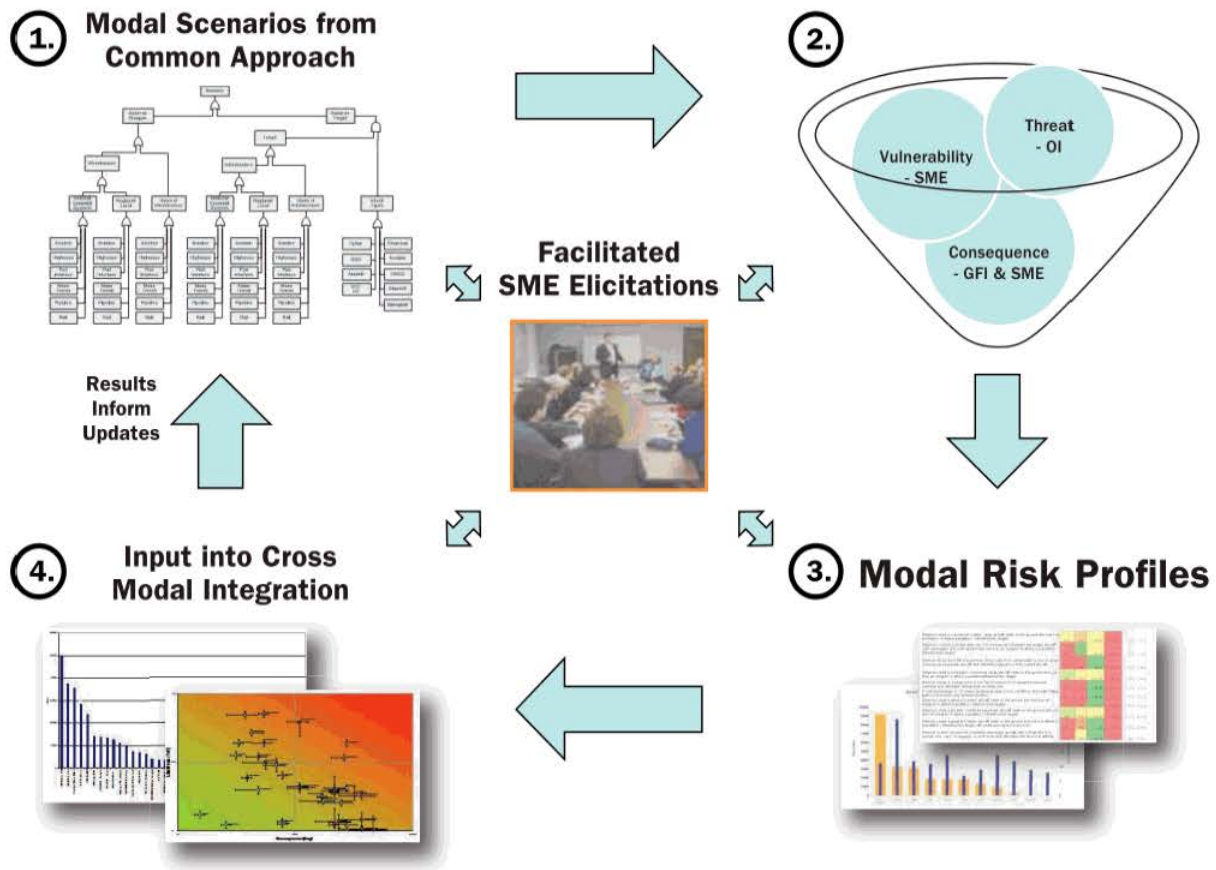
The following are brief descriptions of the primary risk assessment methods used by the six transportation modes along the three class levels. These tools and techniques are not directly mandated by or for specific modes, although some have been developed to fulfill legislative requirements.

Transportation Sector Security Risk Assessment

TSSRA, depicted in figure 3-2, is an example of both a cross-modal assessment (Class 3) and a modal risk assessment (Class 2). It is an analytical technique that ranks the risks associated with multiple attack scenarios in each mode and compares these risks across the sector. TSSRA includes an analysis of the assessment results that suggests risk-based priorities for securing the sector. TSSRA provides a baseline characterization of current levels of risk within and across the transportation modes and provides decisionmakers with a common, defensible analytical framework that allows comparisons across scenarios and modes.

The TSSRA process allows the sector to evaluate scenarios presenting the highest relative risk. This analytical method focuses on a comprehensive set of plausible scenarios including cyber events for different combinations of transportation assets, attack types, and targets via a fault tree analysis. The process includes countermeasure analysis to determine the costs, benefits, and perceived effectiveness of current and proposed countermeasures. Risk scores presented to decisionmakers factor countermeasures in order to provide a better understanding of the usefulness of rankings in identifying cost-effective countermeasure packages. The results of TSSRA will inform decisions about sector priorities.

Figure 3-2: TSSRA's Information Collection Process



Baseline Assessment for Security Enhancement

BASE is a comprehensive security assessment program designed to evaluate posture in 17 Security and Emergency Management Action Items foundational to an effective security program. The assessment results inform security priorities, the development of security enhancement programs, the allocation of resources (notably, security grants), and the compilation of smart security practices for mass transit and passenger rail agencies. BASE is an example of a mission-specific assessment that focuses on vulnerability and effective security implementation. In the BASE program, TSA reviews the implementation of security actions jointly developed by TSA, DOT's Federal Transit Administration (FTA), and sector partners from mass transit and passenger rail systems. The security action items represent a comprehensive update of the Security Program Actions for Mass Transit Agencies that FTA developed following the attacks of September 11, 2001.

BASE 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. TSA implements this continuous improvement process through the Transportation Security Inspectors – Surface who conduct the assessments in partnership with the mass transit and passenger rail agencies' security chiefs and directors. These thorough evaluations have contributed substantially to an elevation in the mode's security posture. For the first time in transportation security, the most effective security practices cited in BASE assessments were shared throughout the transit and rail community, which expanded implementation, and spurred networking among security professionals.

These 17 action items include areas such as: the agency's security plan, background investigation of employees, security training, drills and exercises, public awareness, facility security and access controls, physical inspections and cybersecurity, document control, information sharing, and coordination with other agencies.

Maritime Security Risk Analysis Model

MSRAM is an example of a scenario-based risk assessment that falls into both the modal risk assessment (Class 2) and mission-specific risk assessment categories (Class 1). MSRAM is a risk analysis tool employed by the USCG. Using a combination of target and attack mode scenarios, MSRAM assesses risk in terms of threat, vulnerability, and consequences. As a tool, MSRAM enables Federal Maritime Security Coordinators and Area Maritime Security Committees (AMSCs) to perform detailed scenario risk assessments on all of the maritime CIKR. The maritime mode uses the USCG's MSRAM program to inform strategic and tactical risk decisionmaking. MSRAM is used at all government levels—Federal, State, and local. Significant accomplishments include sharing critical asset identification beyond the transportation systems to 13 CIKR sectors. Decisionmakers are provided with these assessments to aid in risk management decisions. The tool's underlying methodology is designed to capture the security risk facing various targets and assets that span multiple sectors. This allows for comparison among targets, assets, and geographic areas.

As a scenario-based tool, MSRAM evaluates TVC and considers the response capabilities that might mitigate the consequences of an event. The program facilitates operational planning and resource allocation, the National Strategic Security Risk picture for budgeting purposes, prioritization of sector assets, and a risk-based evaluation of Port Security Grant proposals. Expanding the capabilities of MSRAM is an ongoing priority for the maritime mode.

Comprehensive Reviews

Comprehensive Reviews are an example of a Class 1 MASSRA where multiple agencies and local authorities combine expertise to take an in-depth look at a high-risk asset or system in the sector. For example, TSA has conducted Rail Corridor assessments in High Threat Urban Areas (HTUAs) since 2003. These assessments are based on the Hazard Analysis of Critical Control Points method and include participants from the railroads, DOT's Federal Railroad Administration and Pipeline and Hazard Materials Safety Administration, and local responders and law enforcement. The USCG is also adopting the Comprehensive Review approach by leading multi-agency efforts to examine and validate critical maritime infrastructure assessments contained in, or to be added to, the national MSRAM database. DHS uses the Comprehensive Review concept in many critical infrastructure sectors. These include, but are not limited to, the Chemical Sector, the Energy Sector, and on certain dams, levees, and locks on the Nation's waterways. Comprehensive Reviews assess threat, vulnerability, and consequence components of risk and identify critical cyber elements of the systems, and the security practices in place.

3.3 Assessing Consequences

Consequence assessment is the process of identifying and evaluating the potential or actual effects of an event or incident. Assessments occur throughout the sector, both informally and formally. Consequence assessments are conducted at the field, modal, and sector-wide levels and consider physical, human, and cyber elements of critical infrastructure. All consequence assessments consider one or more of the following: health and human safety, economic impact, national security, and cross-sector effects.

3.4 Assessing Vulnerabilities

Vulnerabilities of an asset or system are the physical, cyber, human, or operational attributes that render it open to exploitation or susceptible to hazards. Vulnerabilities are weaknesses that diminish preparedness to deter, prevent, mitigate, respond

to, or recover from any hazard that could incapacitate or disable the infrastructure. The physical, cyber, and human elements of the sector are often co-dependent and additional vulnerabilities may result from their interaction. For example, an intruder overcoming an access control system and gaining entry to a vulnerable cyber control network could cause physical damage or threaten transportation networks. Any assessment should describe the vulnerability in sufficient detail to assist in subsequent development of countermeasures and to facilitate risk reduction. It may include the following:

- Identity of vulnerabilities associated with physical, cyber, or human factors;
- Description of all protective measures in place and their effectiveness; and
- For natural hazards, consideration of the types of harm the incident would cause to determine the vulnerabilities.

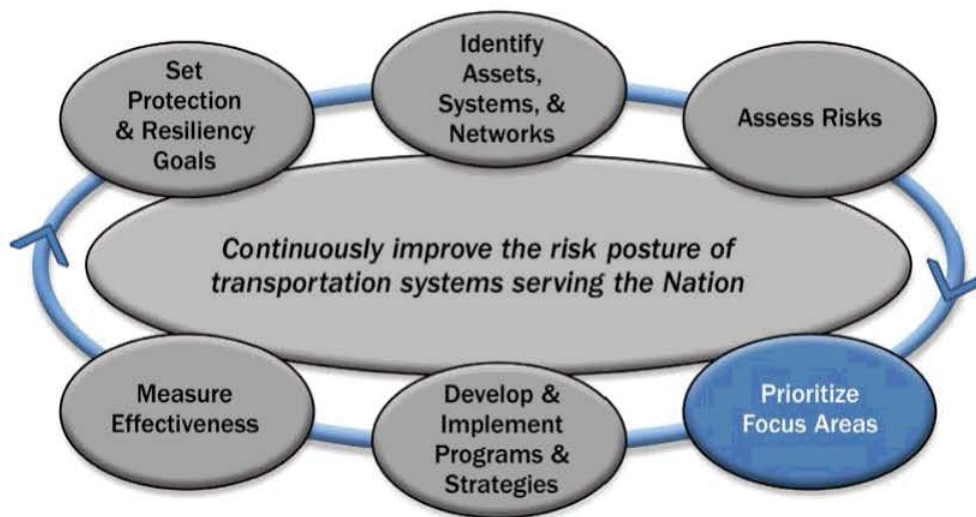
Assessment results should be quantifiable for use in subsequent risk analyses and metrics development.

3.5 Assessing Threats

Threat assessments of manmade or natural disasters are a function of probability based on historical data. The threat of a terrorist attack is determined by an assessment of terrorist capabilities and intents as derived from intelligence analyses. Terrorism threat assessments must consider the degree of uncertainty associated with estimates of capability and intent. Terrorists intend to exploit weaknesses and vulnerabilities by adapting capabilities quickly.

The sector communicates regularly with the U.S. Computer Emergency Readiness Team (US-CERT), the National Cyber Security Division (NCSD), and other IC organizations. The IC provides numerous streams of raw intelligence on physical, human, and cyber elements to SSAs that is then analyzed, filtered, and disseminated to sector partners, as classification and threat levels warrant. The SSAs provide classified and unclassified information to the sector to increase situational awareness and to validate the SSAs' security requirements. These communications are intended to solicit immediate action by stakeholders, especially private sector operational and tactical efforts.

4. Prioritize Focus Areas

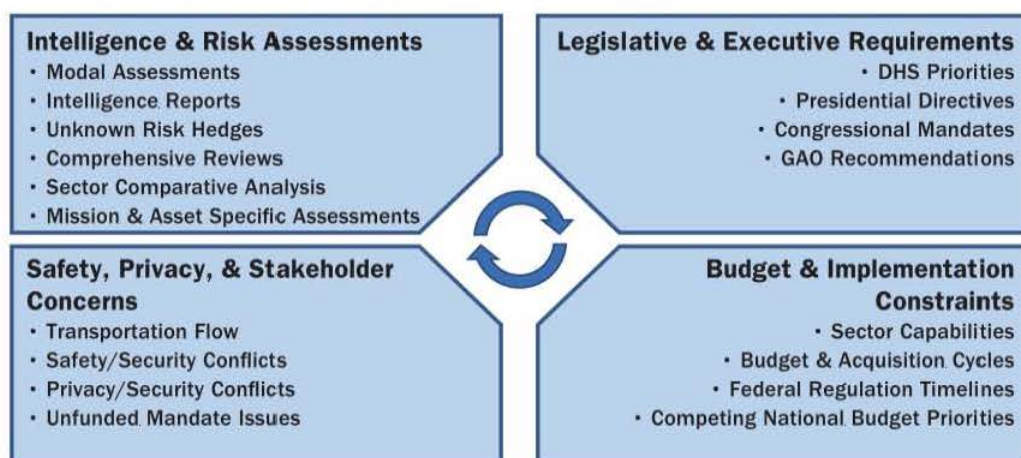


Chapter 3 described how risk assessments based on TVC data are used by the sector to inform resource allocation, as well as strategic and tactical planning. However, while risk assessments provide significant input to resource allocation decisions, other factors must also be considered. Various analytical techniques and tools are employed to gather the necessary data used in the decisionmaking process.

This chapter explains the process by which risk assessment information is analyzed in combination with other factors in the decision environment, to enable the sector to set risk reduction priorities. The prioritization process leads to strategic priorities for the sector with implications for resource distribution and budget submissions. When applied within the mode, the prioritization process determines those aspects of protection and resiliency goals that require specific programming or countermeasure development. Figure 4-1 depicts the overarching categories of the factors that the sector considers when developing protective programs and resiliency strategies.

Owners and operators prioritize critical cyber assets and provide relevant information to the SSAs. The prioritization of critical cyber infrastructure depends on the criticality of the infrastructure it serves and on potential interdependencies between the infrastructure and the critical functions of other sectors. For example, a cyber system that controls food transfer processes between modes of transportation would not be critical to the transportation infrastructure per se, but may be critical to the Food and Agriculture Sector.

Figure 4-1: Inputs into the Development of Protection and Resiliency Priorities



4.1 Intelligence and Risk Assessments

The information gathered from intelligence reports and risk assessments, as described in chapter 3, represents a key factor in the development of programs and strategies. Legislative and executive directives require the SSAs to determine protection and resiliency priorities based on risk. Consequently, these assessments are a major component in determining critical focus areas.

The sector will always face a degree of uncertainty concerning risk, particularly regarding terrorism. Unknown terrorist risk results from terrorists having a virtually limitless range of targets and tactics from which to choose. Terrorists have proven to be adaptive, shifting tactics and strategies in reaction to, or in anticipation of, the mitigating countermeasures the sector develops and implements. While the sector remains focused on known and suspected threats, it also must address risks associated with unknown threats.

A key feature of improving transportation resiliency is striking a balance between countering known risks and hedging against unknown risks. Currently, these hedges involve two strategies: deploying constant and random security countermeasures and enhancing system resilience against all hazards wherever possible and practicable. The sector continues to apply its resources to random, flexible, deterrent initiatives, such as the Visible Intermodal Prevention and Response (VIPR) teams.

4.2 Legislative and Executive Requirements

Working in collaboration with industry experts and State and local government representatives, the legislative and executive branches of the government carefully create policies and regulations intended to benefit and protect society at large. Laws, regulations, and presidential directives may establish priorities independently of the risk management process. These requirements will influence the sector's collaborative decisions regarding sector goals and priorities. HSPD-7 and the 9/11 Act are two examples of such requirements. A complete list of legislation, regulations, and presidential directives is listed in Appendix 3—Authorities.

4.3 Budget and Implementation Constraints

Budgetary constraints or spending limits may influence priority determinations initially. Conversely, the priorities of the sector will influence future government and private sector budget proposals. Enacted budgets (appropriations) may provide immediate

funds to implement legislated priorities. Consequently, the process for determining sector priorities considers fiscal elements in the decision environment for short-term and long-term impacts, in addition to the implications of risk assessments.

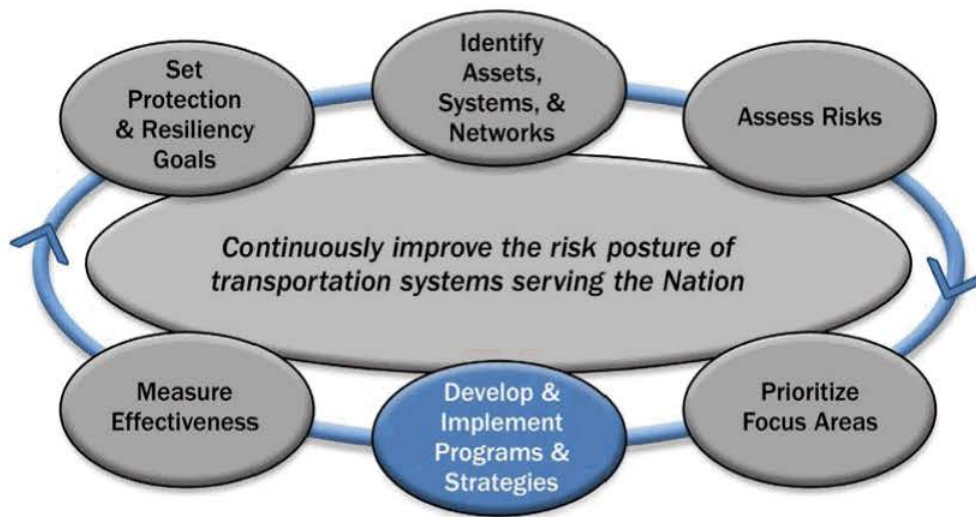
4.4 Safety and Privacy Considerations and Stakeholder Concerns

Stakeholder concerns, safety and privacy considerations,¹⁰ and public opinion are also external factors that the sector does not directly influence. These considerations play a role in defining the sector's responsibilities and capabilities in terms of risk mitigation initiatives. For example, preventing terrorist attacks on critical systems could include procedures that might raise privacy concerns from citizens or sector stakeholders.

¹⁰ Privacy considerations in the form of legislative requirements are also taken into account, for example the Federal Management and Promotion of Electronic Government Services Act of 2002 (E-Government Act).



5. Develop and Implement Protective Programs and Resiliency Strategies



The sector partners collaboratively use the field, modal, and cross-modal risk assessments described in chapter 3 to determine security and resiliency priorities and to develop, implement, and measure protective programs and resiliency strategies based on prioritization. The factors illustrated in chapter 4 play a role in the development of these programs, and include legal considerations, stakeholder input, and budget and time constraints.

This chapter focuses on the methodology used to develop protective programs and resiliency strategies based on the evolving needs of the sector. These programs focus on reducing risks by detecting and deterring threats, preparing for known threats, increasing the sector's overall resiliency, and enhancing preparedness for continuity and recovery operations. In many cases, multiple programs and strategies are layered to reduce the overall risk by mitigating vulnerabilities and subsequently reducing consequences from an incident. Other programs have been developed to address evolving threats. As programs are developed and implemented by various sector partners, they are monitored to ensure continuous improvement. The measurement process is addressed in chapter 6.

5.1 Overview of Sector Protective Programs and Resiliency Strategies

As described in chapter 3, strategic and tactical risk assessments are conducted using TVC data to prioritize security gaps. The sector's protective programs and resiliency strategies are grouped into 12 categories called risk mitigation activities (RMAs).

The RMAs reflect areas that address the sector's strategic goals. Once developed and implemented, these programs are monitored and measured to ensure their effectiveness and efficiency as circumstances evolve. Table 5-1 defines the RMA categorical organization and cites examples of programs currently in place. While the list of programs is not comprehensive, it provides examples of some ways by which the sector mitigates risk.

Table 5-1: Transportation System Sector Risk Mitigation Activities

Key Risk Mitigation Activity	Protective Programs
Security vetting of workers, travelers, and shippers	Transportation Worker Identification Credential (TWIC)
Secure critical physical infrastructure	National Tunnel Security Initiative, Area Maritime, Facility, and Vessel Security Plans (MTSA)
Risk mitigating operational practices	Container Security Initiative (CSI), International Port Security (IPS) Program
Implement unpredictable operational deterrence	Visible Intermodal Prevention and Response (VIPR) Program
Screening workers, travelers, and cargo	Certified Cargo Standard Security Program (CCSP) and Standard Security Program updates
Security awareness and response training	Federal Flight Deck Officer (FFDO) and Flight Crew Member Self-Defense Training
Preparedness and response exercises	Intermodal Security Training Exercise Program (I-STEP), Area Maritime Security Training and Exercise Program (AMSTEP)
Awareness and preparedness	Security Training, Operational Readiness, and Maritime Community Awareness Program (STORMCAP)
Leverage technologies	Electronic Boarding Pass Program, Advanced Imaging Technologies
Transportation industry security planning	Aircraft Operator Standard Security Program (AOSSP)
Vulnerability assessments	BASE Program, General Aviation Airport Vulnerability Assessments
Secure critical cyber infrastructure	US-CERT, NIST, sector-specific programs under development

Key RMAs that are specific to the maritime mode include: Maritime Domain Awareness; Create and Oversee an Effective Maritime Security Regime; Lead and Conduct Effective Maritime Security and Response Operations; and Risk Reduction Tools and Methods.

The SSAs coordinate with sector partners through a variety of security roundtables, monthly or bimonthly teleconference calls, Internet sites, and collaborative exercises. The modal GCC and SCC frameworks are the primary means for collaborative planning, and meet regularly depending on the needs of each mode. Industry associations representing the various modes also offer input during the program development phase of risk mitigation. Chapters 1 and 8 contain additional information on the sector's stakeholder outreach activities.

While the sector recognizes the challenges in quantitatively measuring the success of all protective programs and resiliency strategies, it is committed to demonstrating progress in innovative ways. The sector has developed outcome metrics to serve as progress indicators for various RMA programs, a process that is addressed in chapter 6.

5.2 Determining the Need for Protective Programs and Resiliency Strategies

Once assessments and prioritizations of risks have occurred, analyses are performed to identify needs and to determine progress toward achieving the sector's goals. Additionally, current and potential countermeasures are identified, enabling sector leadership to determine a range of programs that are needed, or to justify current protective programs already in place. Proposed programs consider organizational and sector capability to create effective countermeasures that consider cost effectiveness and value-added protective benefits.

Sector GCC and SCC partners collaborate to identify the capabilities the sector currently has that could be used to mitigate the identified risk. If the capability does not currently exist, the sector will examine other programs (including grants) that may be adapted to address the need, or direct research and development (R&D) activities to design new capabilities, a process detailed in chapter 7. Based on the likelihood that potential vulnerabilities may involve areas where numerous interdependencies are present, the SSAs work with other sectors' SSAs to identify and leverage potential programs as warranted.

During risk assessments, vulnerabilities are identified and analyzed to determine if programs should be developed to reduce the vulnerability, and thereby reduce the overall risk. Often a layered strategy is optimal for mitigating risks and the effects of terrorism, natural disasters, and other manmade incidents. These strategies feature protection and resiliency initiatives spanning multiple jurisdictions, complementary programming, and overlapping security zones.

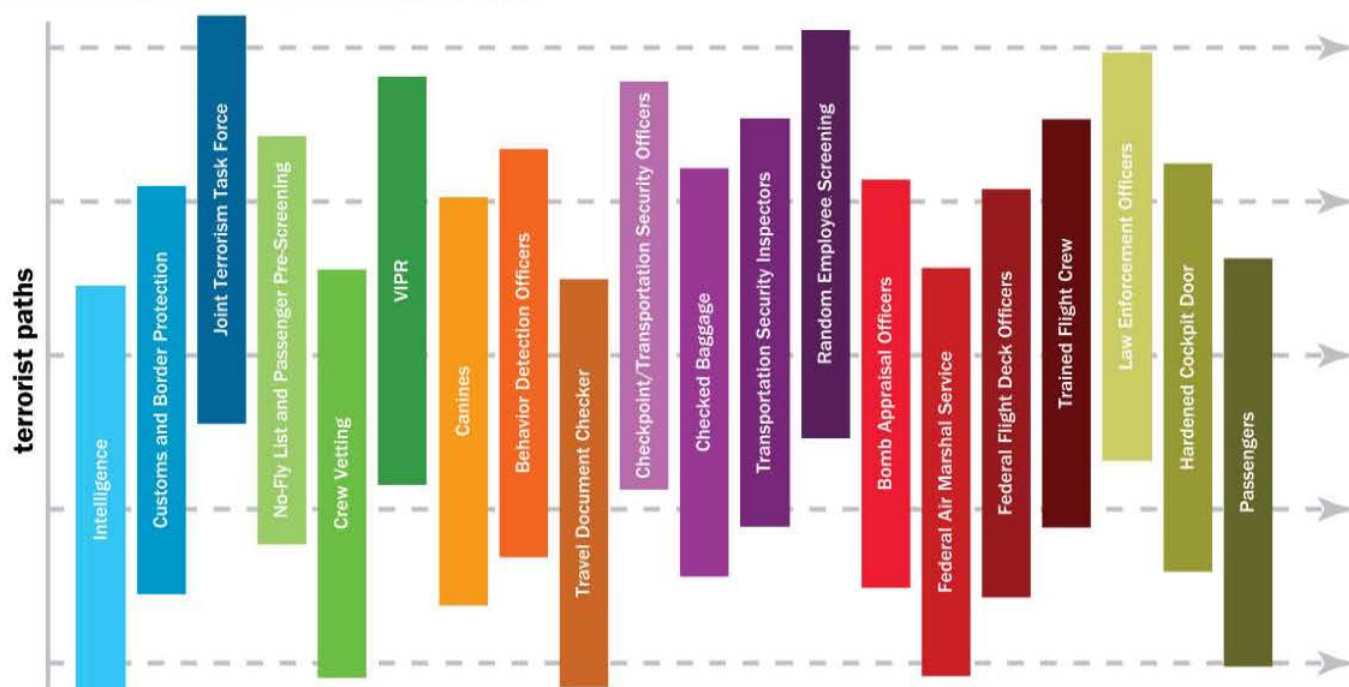
Federal, State, local, tribal, and territorial authorities, as well as the security personnel of owners and operators, provide this multi-jurisdictional layering before, during, and following an incident. A training vulnerability might be addressed through a set of layered training initiatives including entry level, front-line, and security force training conducted through online, classroom, and exercise venues. The sector also draws on an alert, aware, and informed public to contribute to the security posture of the Nation's transportation systems. A mapping of this layering approach in the aviation mode is depicted in figure 5-2.

5.3 Selecting Protection and Resiliency Programs

The selection of a risk reduction approach relies on an understanding of vulnerabilities in critical transportation infrastructure. The consequences attributed to a threat are diminished by changing the vulnerabilities identified in such areas as physical barriers, surveillance, employee training, access controls, cyber elements, or other aspects of security environment. Similarly, threats can be reduced by addressing the vulnerabilities that allow threats to succeed. Therefore, it is important to link vulnerabilities identified in assessments or subsequent analyses to the selection of risk reduction programs.

A variety of analysis methods are available to reach a decision between risk reduction alternatives. One approach is to use a weighted-factor decision method to evaluate programming options. This method allows alternatives to be evaluated based on the extent to which they reduce risks, they are cost effective, and they meet other performance criteria identified by decision-makers. As an iterative process, additional risk assessments may be necessary to understand risk reduction effectiveness of the alternatives being considered.

Figure 5-2: Layered Approach to Aviation Security



Sector partners are responsible for implementing and maintaining their own cybersecurity programs. The SSAs coordinate participation in these programs through the sector's GCC and SCC partnerships and with NCSD. These programs provide online and in-person forums for sector members to share their best practices in IT security. SCCs will play a key role in communicating and implementing new programs to ensure improved resiliency of the Transportation Systems Sector cyber networks.

5.4 Protective Program/Resiliency Strategy Implementation

The implementation phase of the risk management process involves procurement, research, product development, and processes associated with deployment and operations including training and maintenance. This section addresses the establishment of implementation objectives or targets that assist program managers, and the sector, in assessing the effectiveness of programs with respect to performance, cost, and risk reduction. As discussed in chapter 6, the SSAs intend to use metrics to determine the sector's progress in reaching risk management objectives.

As previously stated, programs are selected to reduce risks. Targets are developed collaboratively for protection and resiliency objectives as identified through risk assessments or subsequent analyses. Targets are set for specific vulnerabilities or consequences selected for remediation. In the implementation phase of the risk management process, managers measure or estimate program costs and evaluate progress relative to established targets.

Programming options can include research, development, modeling, and simulation. While implementation of these types of programs does not directly reduce risks, they do fill gaps in capabilities needed for risk reduction. Implementation targets, such as a percentage of project completion or performance criteria, should show the degree to which capability gaps are closed. The joint Transportation Systems Sector Research and Development Working Group (R&DWG) determines R&D priorities, establishes programming recommendations, and monitors implementation of those programs.

The sector's critical cyber systems depend on communications and IT infrastructure—such as the Internet, communication networks, and satellites—for operations and resiliency. With a few exceptions, risk assessments of these systems in several modes are in their infancy and presently do not provide a reliable basis for understanding cyber risks. The sector works closely with other sectors' SSAs and government entities to improve the risk awareness and management processes, identify risks, and implement cyber protection programs. The TSS CWG monitors implementation of cyber risk reduction programs for alignment across agencies and sectors. The working group's members include representatives of NCSD, U.S.-Computer Emergency Readiness Team (US-CERT), Federal transportation agencies, State governments, and infrastructure owners and operators.

Implementation of protection and resiliency programs may impact incident response and recovery networks already in place. For example, system resiliency to all hazards involves many Federal, State, and local jurisdictions with defined roles throughout the event spectrum—prevention, protection, response, and recovery. Budget and resource considerations are also important. For further discussion, see sections 4.2 and 8.2.3. Program implementation should be fully coordinated to assure that existing networks are enhanced. Measurement of programs impacting existing networks may require multiple data points for evaluating network impacts as well as program effectiveness.

The sector will report its progress implementing programs, meeting objectives, and reducing risk in its annual report on critical infrastructure protection and resiliency.

5.5 Monitoring Program Implementation

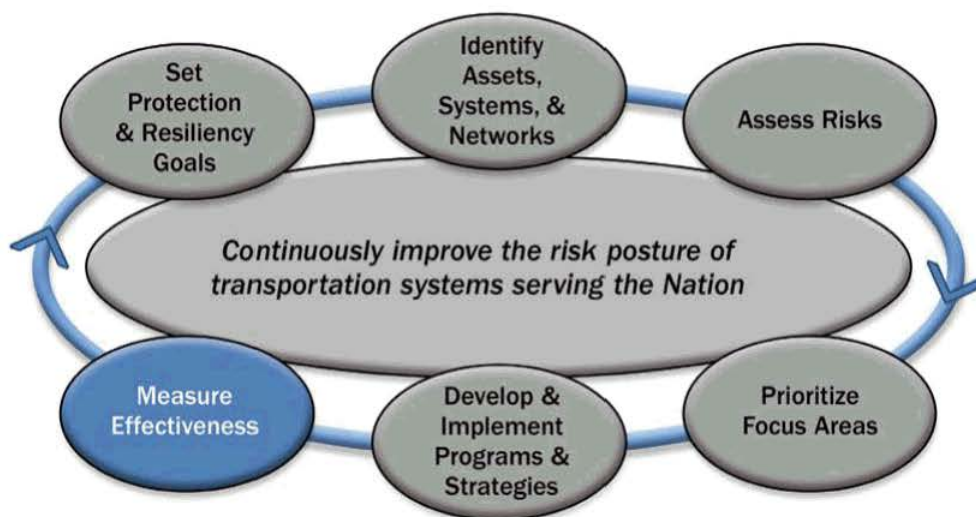
Projects are monitored following implementation. The sector is considering various measures of countermeasure effectiveness. These measures of effectiveness will be used to monitor the degree to which countermeasures achieve their objectives. As these performance measures are identified and documented, the types of data that should be collected to perform the evaluations will also be identified. Output measures will assist in analyzing a program's ability to meet its milestones, while outcome measures will gauge a program's contribution to the sector's risk mitigation objectives.

The sector is improving the implementation of cybersecurity countermeasures, as well as cyber performance measures, through various efforts and with numerous sector partners. The SSAs coordinate cyber protection efforts with the US-CERT through notifications of incidents affecting the sector and by reviewing security bulletins distributed by US-CERT. Other Federal partners and members of the private sector are encouraged to take advantage of the information shared by US-CERT. Furthermore, the SSAs periodically meet with NCSD and the Chief Information Security Officers from various government agencies to develop best practice standards and programs. The SSAs continue to coordinate with NCSD to ensure that the sector's cyber protective programs are aligned with NCSD's cyber priorities and follow protocols developed by NIST and the International Organization for Standardization.

Based on the data requirements and the needs of each program, the sector develops data collection plans for countermeasures. Data collection plans can define what data needs to be collected to update each performance measure, how frequently this data should be collected, and what resources will be required (e.g., analytical tools and methods) to collect the data. During the lifecycle of a given program, output and outcome measures may reveal best practices, improvement areas, and opportunities for management intervention. The monitoring process allows the sector to adapt programs based on changing needs and resources. The performance measurement processes for the sector are discussed in Chapter 6—Measure Effectiveness.



6. Measure Effectiveness



Following comprehensive risk assessments, prioritization, program creation, and program implementation, the effects of these activities are measured. The use of performance metrics is a critical step in the risk management process, enabling the sector to objectively assess improvements in risk reduction, protection, and resiliency. The information gathered in the measurement phase is made available in all other stages of the framework and aids the sector in redefining its goals and objectives as circumstances change. Performance metrics allow progress to be tracked against sector priorities and provide a basis for the sector to establish accountability, document actual performance, facilitate diagnoses, promote effective management, and provide feedback mechanisms to decisionmakers.

As the NIPP metrics process has evolved from descriptive and output data to focus on outcome metrics, the sector's measurement efforts are also moving towards a more outcome- and quantitative-based process. In addition to broad-scope metrics, the development of transportation cyber metrics is being planned in concert with cross-sector teams with a focus on repeatable measurable objectives. Metrics are developed in alignment with NIPP criteria and sector goals, and are used to continuously inform decisionmakers of successes, as well as of areas for improvement.

6.1 Risk Mitigation Activities

The Transportation SSA and Maritime SSA RMA categories represent the strategic focus areas of risk reduction, under which individual, cross-modal, and sector-wide programs and initiatives are aligned. The RMAs organize the key risk reduction programs, initiatives, and strategies and directly support the sector's goals and objectives¹¹ as detailed in section 1.2. This strategic mapping is depicted in tables 6-1 and 6-2.

Table 6-1: Transportation Sector Risk Mitigation Activities Mapped to Sector Goals

Key Transportation SSA RMA	Goal to which Activity Maps			
	Goal 1	Goal 2	Goal 3	Goal 4
Security vetting of workers, travelers, and shippers	✓		✓	
Securing of critical physical infrastructure	✓	✓		✓
Implementation of risk-mitigating operational practices	✓	✓	✓	✓
Implementation of unpredictable operational deterrence	✓		✓	✓
Screening of workers, travelers, and cargo	✓	✓	✓	
Security awareness and response training	✓	✓		✓
Preparedness and response exercises	✓	✓		✓
Awareness and preparedness	✓	✓	✓	✓
Leveraging of technologies	✓	✓	✓	
Transportation industry security planning	✓	✓	✓	✓
Vulnerability assessments	✓	✓	✓	✓
Securing of critical cyber infrastructure	✓	✓		✓

¹¹ **Goal 1:** Prevent and deter acts of terrorism using, or against, the transportation system.

Goal 2: Enhance the all-hazard preparedness and resilience of the global transportation system to safeguard U.S. national interests.

Goal 3: Improve the effective use of resources for transportation security.

Goal 4: Improve sector situational awareness, understanding, and collaboration.

Table 6-2: Maritime Mode Risk Mitigation Activities Mapped to Sector Goals

Key Maritime SSA RMA	Goal to which Activity Maps			
	Goal 1	Goal 2	Goal 3	Goal 4
Maritime Domain Awareness	✓		✓	✓
Risk reduction tools and methods		✓	✓	✓
Create and oversee an effective maritime security regime	✓	✓	✓	
Lead and conduct effective maritime and security response operations		✓	✓	✓

6.2 Process for Measuring Effectiveness

The sector plans to measure effectiveness by collecting data, analyzing, and measuring it against the baselines, or standards, established for programs and initiatives within the RMA categories. Baselines are specific to each type of program or initiative; for example, a baseline measure for VIPR team effectiveness is inherently different than one for an electronic boarding pass program. However, the commonality across programs is that once the baseline measure is established, subsequent deviations from the baseline can be tracked to demonstrate the percentage of change, or improvement, the risk reduction activity has achieved. Information collected must be verified, shared, and stored as appropriate in each case.

While it is feasible to measure and report on progress against stated goals, the sector may never be able to truly rate the effectiveness of some programs. The absence of a terrorist incident or a specific natural disaster does not necessarily mean that the RMAs have reduced a vulnerability that kept the incident from occurring or improved the sector's disaster response capabilities. Where feasible, the sector uses activities such as assessments, exercises, and covert testing to provide some performance data on these types of programs. The sector will continue to work collaboratively with its partners to develop measures, collect data, and report progress as accurately as possible.

6.2.1 Process for Measuring Sector Progress

Measurement progress indicators vary across the sector due to the inherent differences among the transportation modes, and other factors like whether the modes' programs are regulatory or voluntary. While the modes interact with sector partners regularly through informal and formal mechanisms, such as the GCC and SCC, the formal process for working with sector partners to develop progress indicators remains under development. As the sector's measurement process matures, an evaluation will be made to determine whether to reestablish the Measurement Joint Working Group, or to utilize the existing modal GCCs and SCCs as a means to interact with sector partners on metrics-related issues, and to incorporate industry best practice resiliency and recovery metrics.

The responsibility for conducting assessments to measure progress falls on various offices depending on the program or initiative in question, and based on the mode and regulatory or voluntary nature of the program. Some are carried out by the SSAs, DHS personnel, and inspectors such as Transportation Security Inspectors—Surface, while others are conducted by owners/operators or other partner groups. The frequency of assessments is also related to the type of program or initiative. The modal annexes provide more detail in regard to specific measurement and assessment practices.

6.2.2 Information Collection and Verification

Currently, the sector is establishing processes for assessing metrics depending on the specific type. Some processes are internal to SSAs, such as those relating to passenger screening in airports or the Area Maritime Security Plans. Some measurement processes are regulatory, such as the 100 percent cargo screening requirement mandated by the 9/11 Act. Others are based on voluntary compliance, such as vulnerability assessments, while others relate to gaps, such as implementing “next generation” technology solutions. The modal annexes provide more information on assessment and verification processes and frequency, as driven by specific requirements.

Sensitive and proprietary information is protected in accordance with applicable legislation and regulations, such as those governing sensitive security information (SSI). Examples of protections include labeling, storage in locked cabinets, and distribution on a need-to-know basis.

6.2.3 Reporting

Metrics reporting is conducted based on the processes and timelines established by the DHS-led cross-sector NIPP Metrics Working Group and the SAR process. Reporting is provided through the DHS NIPP Metrics Portal and the SAR, as well as other reporting avenues, as required. The SSAs are responsible for reporting and provide metrics based on DHS requirements. Currently, reports are shared with stakeholders through the SAR process. As the metrics process evolves, additional reporting avenues may be explored through the modal GCCs and SCCs.

6.3 Using Metrics for Continuous Improvement

The final step in the NIPP-based risk management framework is using metrics data to inform future plans and decisionmaking efforts to improve sector security and resiliency. Performance metrics evaluate progress against a baseline to determine successes or needed improvements in protection and resiliency programs. A regular data reporting cycle reveals trends that can be used to inform decisionmaking and provides a feedback loop in the risk management process. Establishing performance baselines, determining data collection needs to support established measures, organizing data collection efforts, and evaluating data collected to determine progress that can meaningfully inform decisionmaking for continuous improvement will be an iterative, complex, multi-year process. As the sector’s metrics process matures towards this end, the SSAs will continue to use available program data, intelligence, and subject matter expertise to drive continuous improvement.

The sector’s risk management framework process, from establishing goals to developing risk mitigation strategies and measuring progress, is a continuous one. As progress is made, threats continue to evolve and external considerations gain and lose importance. The sector also engages in activities outside of the risk management framework, such as R&D and building strong partnerships. The final chapters of the SSP describe the SSAs’ additional responsibilities necessary to ensure a secure, resilient, and well-functioning national transportation system.

7. Research and Development

7.1 Overview of Sector R&D

HSPD-7 calls for the Secretary of DHS, in coordination with the Director of the Office of Science and Technology (S&T), to prepare an annual Federal R&D Plan. The National Critical Infrastructure Protection R&D Plan (NCIP R&D Plan)¹² establishes a baseline for R&D capabilities required across all sectors. The NCIP R&D Plan, prepared by the policy division of S&T, highlights the R&D needs as having three primary “technology-enabling” goals and nine technology-centric themes.¹³

Integral to the R&D and S&T processes is the Transportation Systems Sector R&DWG. The R&DWG brings stakeholders together from across the sector to identify mission needs and capability gaps. These needs and gaps are eventually forwarded into the DHS S&T Capstone Integrated Project Team (IPT) Process, which allows multiple Federal partners to collaborate to develop programs and projects that close capability gaps and expand related mission competencies. The sector's goals support the overarching NIPP goal of a safer, more secure Nation. The sector's risk management process provides the foundation for the sector's R&D Plan.

7.1.1 Sector R&D Landscape

R&D has always been essential to the sector and represents an important means to enhance or develop capabilities to deter and prevent terrorist actions. Sector R&D efforts are made more complex and challenging by several factors, including:

- Widely diverse types of infrastructure and operations;
- Inherent vulnerability of surface transportation;
- Constantly evolving threats to transportation; and
- Increasing interfaces and dependencies on intermodal and international transportation.

In addition to ongoing involvement by DHS agencies, continual involvement by the public and private sector stakeholders is also of critical importance in successfully addressing these challenges.

¹² The NCIP R&D Plan can be found on the DHS Web site at www.dhs.gov/xlibrary/assets/ST_2004_NCIP_RD_PlanFINALApr05.pdf.

¹³ The three NCIP R&D technology-enabling goals are: (1) a national common operating picture for critical infrastructures; (2) a next-generation Internet architecture with security designed-in and inherent in all elements rather than added after the fact; and (3) resilient, self-diagnosing, and self-healing physical and cyber infrastructure systems. The nine technology-centric themes are: (1) detection and sensing; (2) protection and prevention; (3) entry and access portals; (4) insider threats; (5) analysis and decision support; (6) response, recovery, and reconstitution; (7) new and emerging; (8) advanced architecture; and (9) human and social.

Sector Asset Ownership Diversity

As previously noted, a large percentage of transportation systems and assets are owned or controlled by diverse public and private sector entities. Such diversity of ownership calls for engagement of all transportation partners in order to expedite the flow of information and appropriately leverage R&D initiatives throughout the transportation community.

The diversity of the sector translates into a wide variety of potential capability gaps that depend on R&D. To organize the R&D initiatives, needs and requirements are grouped into the five Transportation Infrastructure Elements shown in table 7-1.

Table 7-1: R&D Security Needs by Transportation Infrastructure Element

Transportation Infrastructure Element	R&D Related Protection Needs
Transportation Infrastructure, Facilities, and Logistical Information Systems	Protecting physical buildings; securing areas, logistics information, and cyber-based systems, including navigation equipment, air traffic control systems, tracking systems, and communication systems needed to support commerce; securing air/train/bus/metro terminals, bridges, tunnels, highways, rail corridors, all transportation surface structures, pipelines, airspace, coastal waterways, port facilities, airports, and space launch and re-entry sites; protecting railway and transit stations and facilities, rail yards, bus garages, and rights-of-way for tracks, power, and signal systems.
People	Screening passengers for weapons, chemical, biological, radiological, nuclear, and explosive (CBRNE) substances, and other items considered harmful to other passengers and/or the infrastructure, facilities, or transportation equipment.
Baggage Accompanying Travelers	Screening checked and carry-on baggage to protect against weapons, CBRNE, and other items considered harmful to other passengers and/or the infrastructure, facilities, or transportation equipment.
Cargo and Parcel	Screening cargo, parcel, or other shipments using transportation assets within the transportation system to protect against weapons, CBRNE, and other items considered harmful to other passengers and/or the infrastructure, facilities, or transportation equipment.
Conveyance Items and Transportation Equipment	Protecting vehicles for surface, water, or air, including airplanes, buses, trains, trucks, boats, and other vehicles that transport people, services, or goods.

Constant Evolution of Transportation Security Threats

One of the primary characteristics of the transportation security environment is constant evolution of threats. The terrorist threat poses special challenges since terrorists are highly adaptive, seeking to learn and adjust their strategies based on past responses. Terrorists look for ways to defeat or get around current security measures by adapting to changes in countermeasures. A measure of unpredictability must be built into operations and capabilities so terrorists cannot use consistency to their advantage in planning an attack. Therefore, R&D approaches should be based on breadth of application, flexibility, and/or unpredictability.

Increasing Interfaces and Dependency on Intermodal and International Transportation

Driven by the increased mobility of today's society and the expansion of commerce domestically and globally, holistic intermodal preparedness planning is required across all transportation modes. First, similar R&D efforts need to be leveraged across modes. Second, travel or commerce transactions that span multiple transportation modes need analysis, coupled with

comprehensive R&D programs, to minimize security exposures during handoffs between domestic and international transportation modes.

Cyber systems, including air traffic control, tracking, and communication systems needed to support commerce, provide a fundamental capability in keeping the Nation's transportation system safe and operational, especially given growing foreign dependencies. The growth in shipment volumes into the United States from foreign ports and borders calls for R&D to solve multiple challenges to minimize impediments to international commerce, while maintaining safety and security measures. The development and implementation of common approaches to critical infrastructure protection and response to terrorist incidents is important to U.S. security. R&D efforts that support cross-border programs must rely on common definitions, standards, protocols, and approaches in an agreed-upon, coordinated fashion to be effective.

7.1.2 Sector R&D Partners

The key partners and stakeholders in the R&D community are:

- SSAs: TSA and USCG;
- DHS, to include IP and S&T;
- DHS components, to include CBP and FEMA/Grants & Training;
- Interagency partners such as: DOT, DOS, DoD, and DOE;
- State, local, tribal, and territorial organizations;
- Private sector owners, operators, and research entities; and
- Academia, national laboratories, and other research centers, including international entities.

7.1.3 R&D Alignment with Sector Goals

Drawing from the sector's goals and the technology-enabling vision of the NCIP R&D Plan, the sector's R&D Plan will focus on the following strategic goals and aligned objectives:

Table 7-2: Alignment of Sector Goals and R&D Objectives

Sector Goal	R&D Aligned Strategic Objectives
Prevent and deter acts of terrorism using, or against, the transportation system.	Develop and deploy state-of-the-art, high-performance, affordable systems to prevent, detect, and mitigate the consequences of CBRNE and cyber attacks on the sector.
Enhance the all-hazard preparedness and resilience of the global transportation system to safeguard U.S. national interests.	Improve materials and methods to increase the strength and resilience of critical infrastructures for integration into new construction, facility upgrades, and new or upgraded transportation structures (e.g., tunnels, highways, bridges, pipelines, conveyance vehicles, and cargo containers). Design dynamic, self-learning transportation network systems with tightly defined permissions for secure data access within a common operating picture. Develop equipment, protocols, and training procedures for response to, and recovery from, CBRNE and cyber attacks on the sector. Develop methods and capabilities to test and assess threats and vulnerabilities, prevent surprise technology, and anticipate emerging threats.

Sector Goal	R&D Aligned Strategic Objectives
Improve the effective use of resources for transportation security.	<p>Develop technical standards and establish certified laboratories to evaluate homeland security and emergency responder technologies, and evaluate technologies for SAFETY Act protections.</p> <p>Develop ongoing cross-pollination activities (testing, studies, pilots, etc.) between government and stakeholder partners to expand the pool of available technologies to enhance security.</p>
Improve sector situational awareness, understanding, and collaboration.	<p>Increase awareness of the R&D capabilities available for threat-deterrent actions through stakeholder outreach programs, more timely publication of R&D studies and findings, and information sharing.</p> <p>Develop layered, adaptive, secure nationwide enterprise architectures to facilitate shared situational awareness to enable real-time alerts to threats at an operational level.</p> <p>Align sector resources and identify a security-relevant transportation R&D portfolio that assists in prioritizing high-need R&D efforts that may include developing common definitions and nomenclature.</p>

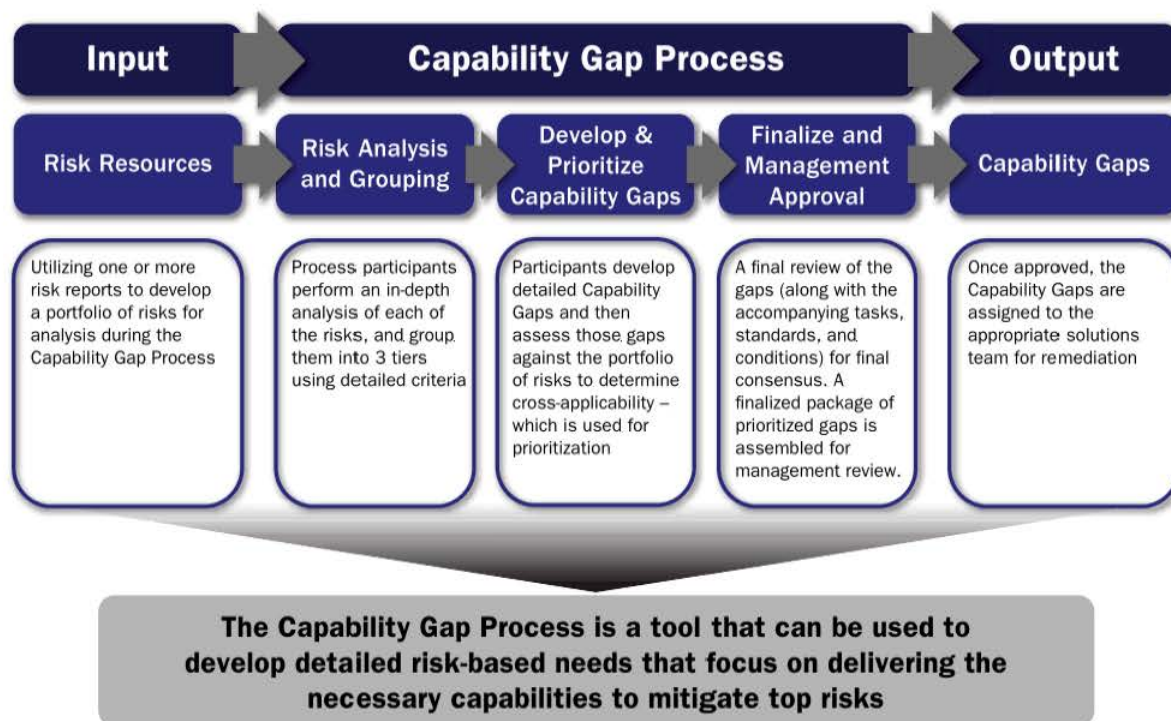
7.2 Sector R&D Needs

The cyber capabilities gap identification process relies on the implementation of the risk management framework in each mode to identify critical cyber systems and to determine needed capabilities. The sector is initiating the process for cyber risk management and will identify capability gaps as that process indicates.

7.2.1 Using the Capability Gap Process to Develop R&D Programs

A capability gap represents the difference between a current capability and the capability required to mitigate risks and other operational needs. A well-defined capability gap forms the basis for R&D projects. The Capability Gap Process allows the sector to identify and prioritize capability gaps that take into account risks, mission goals, and current capabilities. Sound inputs and the credibility of process participants are the foundation of the Capability Gap Process. An overview of the process is depicted below in figure 7-1.

Figure 7-1: Capability Gap Process



Process Inputs

To develop risk-based requirements, the Capability Gap Process uses information from multiple risk and vulnerability reports. Multiple resources are used to provide different perspectives while minimizing the possibility of analytical error. Once the top risks are selected, they are presented for evaluation.

Capability Gap Process

The Capability Gap Process consists of three stages to discuss and evaluate risks, develop a comprehensive and prioritized list of capability gaps, and create a finalized package for management review and assignment. As a result, the process will yield a final set of risk-based capability gaps and initial requirements for solution development.

Risk Analysis and Grouping

Since all of the risks presented are designated as High, there is a need to rank these risks using more detailed criteria.

Each risk is mapped to a nodal diagram depicting the path of attack an adversary would likely follow. The attack path may also highlight other information such as current countermeasures, and previously identified capability gaps (where a solution may already be under development). After reviewing each nodal diagram and risk description, the risks are grouped using the following criteria:

- Magnitude of Consequence: Refers to a particular risk/threat scenario's perceived consequence (loss of life, social, and economic impacts) if an attack is carried out successfully. This is measured on a Tier I, Tier II, Tier III scale.
- Adversary Resource Requirements: Refers to the complexity of effort required by the attacker to exploit a specific risk. This is measured on a Simple, Moderate, Complex scale.

- **Professional Judgment:** Refers to the personal judgment of process participants who have expertise in the field. These judgments are rated as Grave, Concerned, or Low Concern.

Finally, the risk groups are analyzed and described in terms of capability gaps.

Develop and Prioritize Capability Gaps

Next, each capability gap is reviewed, assessed, and refined for comparative evaluation in the prioritization process. During prioritization, the types of risks and the number of risks covered are considered. For example, a greater importance is placed on capability gaps that span multiple, higher-level risks than those gaps that span fewer or lower level risks. The capability gap-to-risk analysis determines the gap's priority as High, High-Medium, Medium, Medium-Low, or Low.

Finalize Capability Gaps and Prepare for Management Approval

Finally, the top priority capability gaps are validated and reviewed for accuracy and completeness prior to submission for management approval. Once approved, the tasks, standards, and conditions of each capability gap become the initial requirements for solutions development.

7.2.2 Defining Sector R&D Needs

The R&DWG will enable collaboration across all stakeholders to identify and maintain the R&D-related requirements and capabilities that the sector currently has identified to continue to mitigate identified risks. Since R&D is a shared activity across the Federal Government and private sector, a great deal of insight and expertise is harnessed to help develop the appropriate technology needs. Many of these needs will be addressed through normal planning and programming activities, and are communicated to the R&DWG for inclusion in the SAR which reflects the sector's requirements, capability gaps, and mission needs for DHS consideration.

Some of the risk-based sector technology needs are:

1. Enhance screening effectiveness for passengers, baggage, cargo, and materials for the six modes of transportation within the sector:

- Incorporate screening for CBRNE;
- Increase throughput, improve detection, lower false alarm rates, reduce staffing requirements, improve operational effectiveness, and provide cross-modal capability;
- Exploit recent advances in biotechnology to develop novel detection systems and broad spectrum treatments to counter the threat of engineered biological weapons;
- Develop transformational capabilities for stand-off detection of special nuclear material and conventional explosives; and
- Explore environmental factors that reduce screening effectiveness and develop programs that mitigate those factors, and improve the effectiveness of current security assets.

2. Enhance infrastructure and conveyance security:

- Improve detection and deterrence, including integration of biometric-based systems;
- Incorporate “security by design” into infrastructure and systems. Develop design guidance and risk mitigation strategies for integration into infrastructure and facilities;
- Develop improved materials and methods to increase the resilience of infrastructure;
- Improve and enhance container and vehicle tracking;

- Provide secure authentication and access control;
- Develop quick and cost-effective sampling and decontamination methodologies and tools for remediation of biological and chemical incidents;
- Explore biometric recognition of individuals for border and homeland security purposes in a rapid, interoperable, and privacy-protective manner; and
- Recognize and expedite safe cargo entering and leaving the country legally, while securing the borders against other entries.

3. Improve information gathering and analysis:

- Provide an integrated view of available incident information;
- Increase domain awareness by providing dynamic situational awareness and analysis;
- Develop risk analysis and situation simulation models for assessing and evaluating mitigation and response/recovery strategies; and
- Develop an integrated predictive modeling capability for chemical, radiological, or nuclear incidents, and collect data to support these models.

4. Provide a common operating picture for transportation systems:

- Develop adaptive, self-healing, secure, and interoperable enterprise architectures;
- Incorporate resiliency into networks and systems; and
- Establish data standards that facilitate a common operating picture.

5. Implement needed cybersecurity capabilities:

- Protect sensitive information generated and housed on security screening equipment and the telecommunications networks used to interconnect them;
- Ensure the accuracy, completeness, and availability of IT systems;
- Provide training to employees to make sure they are aware of how to properly handle sensitive information, including applicable laws and regulations; and
- Guarantee the availability of information and services and put into place the required business continuity and contingency planning.

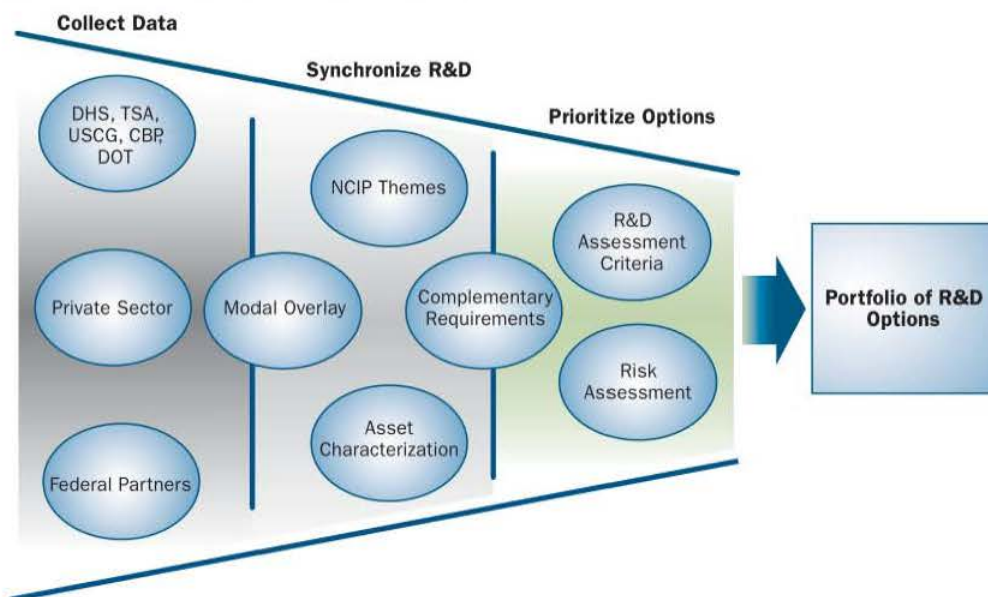
7.3 Sector R&D Plan

The R&D Plan focuses on advances in science and technology, and improving operational and human performance levels, in support of achieving sector goals.

7.3.1 Components of the Sector R&D Plan

The R&D Plan has two primary parts. The first part is designed to meet the sector goals, and describes the portfolio of existing initiatives that are designed to respond to specific requirements within the sector. It includes R&D programs from the public and private sector. The second part of the plan focuses on new initiatives that meet the emerging and ongoing requirements of the sector. Figure 7-2 illustrates the process for developing the R&D Plan.

Figure 7-2: Transportation Systems Sector R&D Plan Process



7.3.2 Sources of Input to the Sector R&D Plan

To produce the R&D Plan, an initial review of transportation security R&D programs was conducted. Sources for this preliminary review include:

- TSA
- USCG
- OSTP
- S&T
- DOT
- CBP
- NIST
- National Science Foundation (NSF)
- National Academies of Science-Transportation Research Board (TRB)

The R&D Plan incorporates input from R&D programs from academia, the private sector, and other Federal, State, local, and tribal governmental entities to complete required data.

7.3.3 R&D Portfolio Framework

The NCIP R&D Plan is structured around the nine R&D themes that support all 18 critical infrastructure sectors. The nine themes were identified as the concerns of infrastructure owners and operators, industry representatives, and government officials. These themes include:

- Detection and Sensor Systems
- Protection and Prevention

- Entry and Access Portals
- Insider Threats
- Analysis and Decision Support Systems
- Response and Recovery Tools
- New and Emerging Threats and Vulnerabilities
- Advanced Infrastructure Architectures and System Designs
- Human and Social Issues

The R&D framework provides a common language and reference point that allows the comparison of R&D programs and enables the formulation of a strategic way forward. The framework does not dictate individual agency budget considerations or requirements.

Current Federal transportation security R&D initiatives have been mapped against the nine NCIP R&D Plan themes and associated sub-themes as a first step toward developing the baseline R&D portfolio. Particular emphasis was placed on identifying cross-modal programs for the sector. The R&DWG will continue the process of identifying sector partners' current and planned R&D initiatives against the NCIP R&D Plan themes to assist in identifying strategic gaps in research and requirements.

Once the final framework is established and agreed upon, the R&DWG can develop summary conclusions about sector R&D programs, including:

- Strengths and goal coverage
- Cross-modal capabilities and potentialities
- Complementariness and interdependence of programs
- Opportunities for collaboration

7.3.4 Technology Transition Through the R&D Life Cycle

The phases of research and development required to bring potential technologies to full maturity and to address one or more security challenges include:

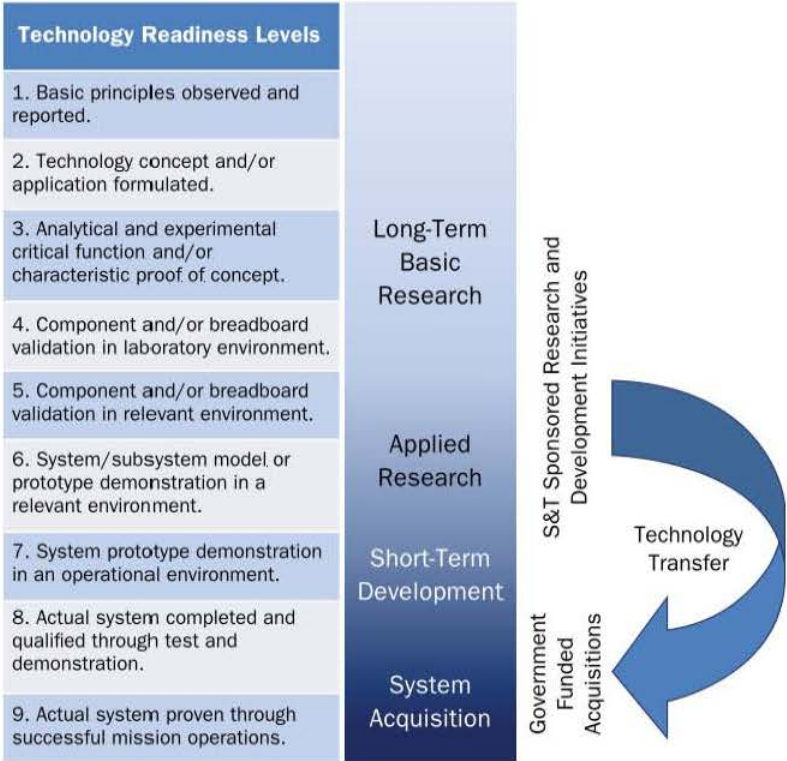
- **Basic Research**—The sector looks to the national laboratories and academia to complete long-term basic research. S&T utilizes the expertise of nine national laboratories under Section 309 of the HSA of 2002. Academia has been directly engaged through a number of activities, ranging from the funding of university-based research centers, such as the DHS S&T Centers of Excellence and Cooperative Centers and DOT Research and Innovation Technologies Administration's (RITA) University Transportation Centers, to direct funding of specific research programs.
- **Applied Research**—S&T also sponsors applied research and early-stage pilot test and development activities. Applied research is necessary to bring concepts to a level of maturity necessary to transition to the development of a full-fledged set of products or processes. Funding and/or support from the government and private sectors are necessary beyond this point to bring products to a commercially viable state.
- **Short-Term Development**—The objective of these types of initiatives is to design and implement incremental improvements to system/sub-system prototypes that are near operational-ready status. In the past, both S&T and the SSAs have sponsored short-term development efforts.
- **System Acquisition**—Systems based on technologies that have been proven to work in their final form, and under expected or mission conditions, can be considered for procurement. This represents the end of R&D and includes developmental tests and evaluations of the system in its intended system configuration to determine if it meets design specifications, or is

using the system under operational mission conditions. Systems based on these technologies are candidates for acquisition and deployment.

Each technology may require a different path to maturation due to the uniqueness of the technology and the specific requirements of the transportation modes. The objective is to allow technologies to develop and mature. During this process, the viability and applicability of each technology is assessed and evaluated. As a result, only those technologies that continue to show viability can be identified and further pursued, and eventually procured.

As shown in figure 7-3, this progress can be further described using the nine DHS Technology Readiness Levels. This figure also highlights the transition of a technology, which has proven to be viable and is sufficiently mature, from S&T to the SSAs.

Figure 7-3: Technology Transition Through the R&D Life-Cycle



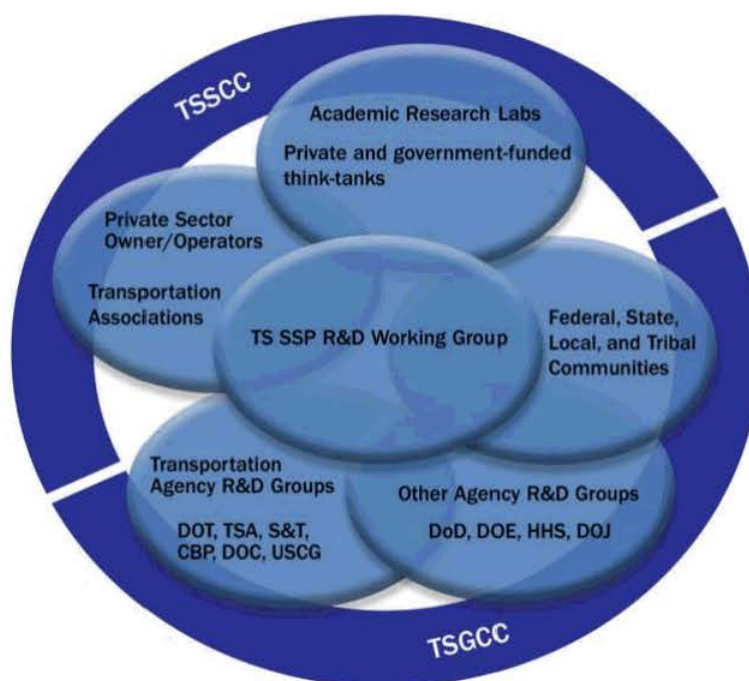
7.4 Sector R&D Management Process

7.4.1 Sector R&D Governance

Under the leadership of the SSAs and the sector GCCs and SCCs, the R&DWG collaborates with sector partners to identify the R&D-related capabilities the sector currently has that could be used to mitigate any identified risks.

Figure 7-4 illustrates the interconnected relationship of the sector R&D community.

Figure 7-4: Interconnected Transportation Systems Sector R&D Community Relationships



7.4.2 Sector R&D Working Group

The R&DWG is comprised of Federal, State, local, tribal, and territorial government representatives, as well as private sector partners and academia. The R&DWG works closely with, and serves, the sector and modal GCCs and SCCs as established in the SSP. The R&DWG serves all transportation modes as its scope of focus, with a particular emphasis on multi-modal issues and cross-sector dependencies, where greater planning gaps may exist.

The primary mission of the R&DWG is to identify mission needs and capability gaps for the sector. The ultimate intent is to align efforts across all stakeholders, better articulate the R&D process, and provide a common focal point for documenting research and development efforts across the sector to strengthen resilience against threats to the system.

The strategic objectives of the R&DWG are to:

- Harmonize transportation R&D efforts for assets, systems, and networks by identifying currently available technology and complementary programs, facilitating common definitions and standards, and disseminating best practices;
- Build consensus for collaborative planning processes and execution with all sector stakeholders; and
- Engage and encourage efficiencies in sector R&D through greater awareness and communication by implementing data sharing across sector agencies and stakeholders.

The R&DWG will determine the scope of continuing management and processes for the group, such as objectives; primary and secondary participation composition; and operational guidelines, such as the time commitments required for participants from sponsoring agencies and rules of engagement.

R&D efforts are derived using a technology scan and transition approach. From these efforts, a broad set of requirements are submitted to S&T for short, medium, and long-term desired outcomes. Through the DHS S&T Capstone IPT Process, the SSAs and S&T are able to develop technology requirements for funding and coordinate requirements with other DHS stakeholders to

eliminate duplication of effort and share experience and knowledge. The SSAs, S&T, and industry representatives also participate in bi- and multi-lateral international meetings and working groups that focus on information sharing about a specific technology or broad technology needs and requirements. The path results in either a basic, applied, or advanced research program, or some combination thereof. The goal is to build a partnership between the public and private sector, so that R&D initiatives can be quickly, safely, and cost-efficiently integrated into operational environments in parallel with advanced research aimed at new and emerging threats.

7.4.3 Coordination with the Critical Infrastructure Protection R&D Community and Other Sectors

Through the CIPAC, the R&DWG will work to provide input and guidance to the developers of the NCIP R&D Plan and other R&D government transportation security planning efforts. The R&DWG, within its CIPAC charter, includes the private sector and other nongovernmental members involved in the sector or R&D community to collaborate in the development of the working group charter, documentation, and deliverables. The goal of private sector involvement is to ensure stakeholder participation to achieve commonly defined protection goals and to foster collaboration that accelerates R&D capabilities to more rapidly satisfy sector requirements. The private sector is equally responsible because its ownership of a significant percentage of transportation assets gives it a critical role in implementing transportation protection and resiliency initiatives. The R&DWG recognizes that the initiatives developed by the government must be closely coupled with the operational goals and requirements of the private sector to be effective.

7.4.4 Progress and Impact of the Plan

The DHS S&T Capstone IPT and derivative project teams and working groups enable multiple constituents within DHS and other Federal sector representatives to come together and provide management oversight of cost, schedule, and technology development performance. It is a continuously evolving process designed to respond to the identified Enabling Homeland Capabilities.

7.4.5 Technology Scanning and Technology Transition

Technology scanning and technology transition are also part of the S&T Capstone IPT process. As an example, the Transportation Security Capstone IPT has the following responsibilities:

- Identify, assess, and prioritize capability gaps relating to the Transportation Security Capstone IPT's mission area;
- Assess feasible solutions proposed by S&T as technology solutions, assuring that these technology solutions properly address capability gaps and demonstrate affordable and significant impacts on homeland security;
- Prioritize technology solutions and select those to be executed within the Capstone IPT's allocated budget;
- Ensure that Project IPTs are formed and chartered to oversee project execution;
- Ensure that Project IPTs develop and coordinate requirements, technology development strategies, and technology transition strategies;
- Ensure that Project IPTs execute Technology Transition Agreements;
- Review progress of Project IPTs to ensure that technology is developing on schedule and is aligned to customer requirements and acquisition plans;
- Review and approve Technology Transition Agreements; and
- Provide concurrence and support on the funded capability gaps and technology solutions after a Capstone IPT investment decision has been made.

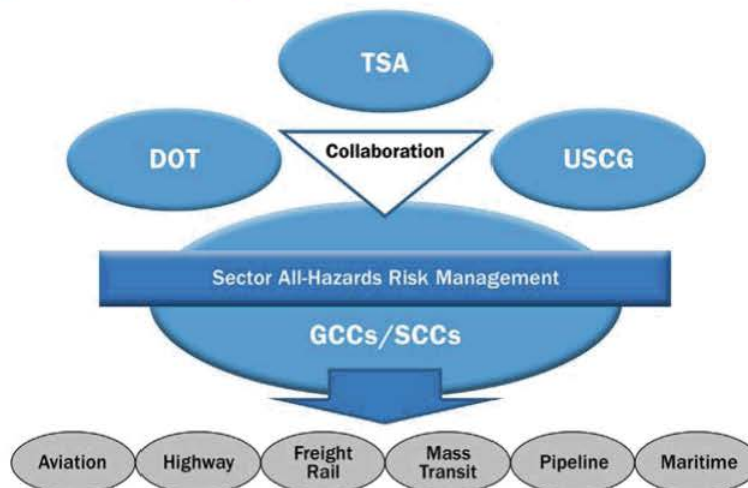
8. Managing and Coordinating SSA Responsibilities

Chapter 8 describes the management approach and the processes applied within the sector for achieving the vision, mission, and goals as laid out in chapter 1. The SSAs oversee the implementation of these processes through the participation of the sector's partners in the development of the sector's goals, determination of protection and resiliency priorities, annual review of the priorities and the SSP, and preparation of the SAR.

8.1 Program Management Approach

As previously discussed, the sector is led by two SSAs who share risk management responsibilities over the six transportation modes. The SSAs perform these responsibilities as depicted in figure 8-1. The USCG chairs the Maritime Modal GCC and the TSA modal offices chair their respective modal GCCs. The sector-wide and modal GCCs and SCCs work with Federal, State, local, tribal, and territorial sector partners and industry stakeholders to plan, develop, and implement infrastructure protection and resiliency activities for all hazards.

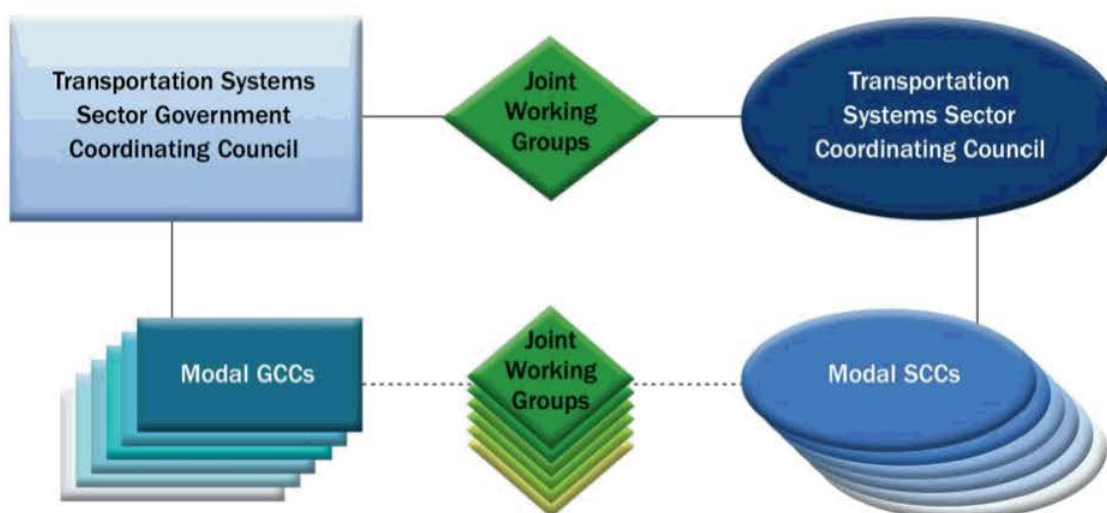
Figure 8-1: Transportation Systems Sector Management Approach



8.2 Implementing the Sector Partnership Model (SPM)

Figure 8-2 depicts the Transportation Systems SPM, featuring the sector GCC and SCC and six modal GCCs and SCCs. This conceptual partnership model is largely in place; however, some adaptations have been made and some elements are yet to form. Several modes have active advisory committees chartered under FACA that also provide security advice to Federal managers. Other modal partnership forums provide a regional voice for security concerns. For example, the Maritime SSA uses the Area Maritime Security Committees within each Captain of the Port Zone to collaborate with stakeholders in the port. The sector focuses on the CIPAC-based partnership model due to its flexibility and adaptability to form working groups to address the collaborative activities of the risk management framework.

Figure 8-2: Implementing the Sector Partnership Model



Joint working groups have been established for collaboration in cross-modal research and development and cybersecurity. Joint working groups are being considered for risk assessments and analyses, information sharing, and metrics. This partnership approach meets legislative requirements for collaboration among government and industry partners to assure effective exchange of information, set priorities, and develop effective solutions to protection and resiliency risks.

Supporting the Transportation Systems SPM are modal and sector-specific ISACs that foster collaboration between government and private sector stakeholders. A planned Transportation Security ISAC will collect and distribute threat, vulnerability, and incident information efficiently and broadly across the sector. This effort is supported by the existing Surface Transportation, Public Transit, Highway, Maritime, and Research ISACs, which gather modal-specific information for dissemination to their immediate stakeholder groups and to the membership of the Transportation Security ISAC. These partnership mechanisms allow for the protected flow of information between government and private stakeholders on a daily basis.

8.3 Processes and Responsibilities

8.3.1 SSP Maintenance and Update

The SSAs are responsible for maintaining and updating the SSP. The SSP and the modal annexes are reviewed annually by the sector's GCC and SCC members and other sector partners. When updates are indicated, the SSAs work through DHS IP to publish amendments or errata, as appropriate. The SSP is rewritten on a three-year cycle through a collaborative process involving the GCCs and SCCs for the sector and the modes.

Progress implementing the SSP is evaluated and reported annually in accordance with DHS IP guidance. The SAR contributes to the development of the National CIKR Protection Annual Report (NAR) and is one of 18 sector reports appended to the NAR. The NAR is submitted to the White House and to Congress.

8.3.2 SSP Implementation Milestones

Table 8-1: SSP Risk Management Milestones and Way Forward

Risk Management Framework	Milestones (in light blue)
	Way Forward (in dark blue)
Set Protection & Resiliency Goals	<ul style="list-style-type: none">• Conduct annual review and validation/update based on process feedback• Update modal cybersecurity objectives for modal specific and intermodal concerns
	<ul style="list-style-type: none">• Communicate goals and objectives to the sector• Sponsor voluntary establishment of a sector-level SCC• Review transportation goals and objectives of State homeland security advisors and other jurisdictions during SSP review process
Identify Assets, Systems, & Networks	<ul style="list-style-type: none">• Participate in annual DHS NCIPP and the Critical Foreign Dependencies Initiative
	<ul style="list-style-type: none">• Refine the sector CIKR identification process to include recognition of critical cyber systems• Establish criteria for considering intermodal consequences in identifying critical infrastructure• Encourage owners and operators to provide asset information to sector infrastructure databases
Assess Risks	<ul style="list-style-type: none">• Refine the sector strategic risk assessment model for the annual risk assessment requirement
	<ul style="list-style-type: none">• Develop modal risk assessment models for critical cyber systems• Define data elements for the sector data repository to support risk assessments• Incorporate sector compliance and assessment data into sector database
Prioritize Focus Areas	<ul style="list-style-type: none">• Update priorities based on annual assessments
	<ul style="list-style-type: none">• Develop processes for analysis and prioritization of cyber risks• Develop process to determine protection and resiliency lessons-learned during incidents and to apply them to prioritization decisions

Develop & Implement Programs & Strategies	<ul style="list-style-type: none"> • Update the Transportation Security Information Sharing Plan (TSISP) annually • Consult non-profit employee representative organizations regarding the SSP • Incorporate all-hazards considerations in capability gaps analyses
	<ul style="list-style-type: none"> • Improve participation of agencies and sector partners in the Transportation Systems Sector R&DWG • Establish the Transportation Security ISAC • Increase awareness of criticality of cyber systems to transportation operations • Conduct pilot of cybersecurity risk management approach • Issue regulations as authorized to implement the 9/11 Act
Measure Effectiveness	<ul style="list-style-type: none"> • Work with government partners and DHS IP to meet the NIPP's annual metrics milestones
	<ul style="list-style-type: none"> • Develop data streams to determine risk reduction effectiveness of protection and resiliency programs • Participate in the SAR process

These milestones complement legislative mandates, which may be implemented through regulations, as mentioned in the authorities section of chapter 1 and in Appendix 3—Authorities. New milestones are added as needed, and developed as a result of identified vulnerabilities.

8.3.3 Resources and Budgets

Each of the sector's partners contributes to resourcing the activities which address the protection and resiliency objectives for transportation systems. As priorities are determined and risk remediation options are considered, the SSAs' modal leaders discuss threats and vulnerabilities with stakeholders through the partnership framework. Security priorities are established through several mechanisms to apportion limited resources and funds in the most effective way. First, the President and Congress establish policy and budget priorities through directives and legislation. Second, sector priorities are established through annual risk evaluations and program reviews, such as TSSRA and the SSP annual review, with results reported in the SAR. Third, critical infrastructure is identified and reviewed annually through the NCIPP.

Federal resources include field personnel for screening, inspections, compliance audits, assessments, law enforcement, and explosives detection (e.g., canine units). In addition, Federal funding, as authorized, is available to sustain protection and resiliency-related programs and operations, such as cargo screening initiatives, VIPR operations, training and education projects, equipment testing, and security exercises. Federal departments can use operating funds to support emergency response consistent with authorities and missions. FEMA also funds Federal, State, and local agencies that provide support during declared emergencies for expenses exceeding normal mission responsibilities and budgets. Federal grant funds are available to transit agencies, Amtrak, rail lines, trucking companies, intercity bus operators, ports, and certain aviation operations, as authorized, for transportation security projects. Additional homeland security grant funds are available for first responders and other response and recovery preparedness activities in States, localities, and tribal areas. DOT also administers a number of grant programs for infrastructure improvements that often benefit the homeland security mission by creating more resilient structures or operations.

The States have the opportunity to identify critical infrastructure for consideration in programming and budgeting processes. Security priorities within the States influence appropriations legislation through the political process, sector priorities through sector risk analyses and planning, and security programming (including grant proposals) through the coordinating aspect of State budgeting processes. State and local governments fund, staff, or otherwise resource emergency operations facilities; maintain emergency response units, law enforcement personnel, and fire fighters; and assure all-hazard training and preparedness for their workforce, industry, and the public.

The owners and operators of the sector's critical assets, systems, and networks contribute immeasurable resources to transportation security and protection activities. They bear a large share of the protection and resiliency responsibilities. Consequently, the sector strives to minimize costs, while maximizing benefits of risk management activities necessary to protect infrastructure, people, and cargo in order to assure system resiliency.

8.3.4 Training and Education

The sector's training and education initiatives consist of online and residence courses, modal or infrastructure specific educational materials, on-the-job training, and exercise and drill programs. Each mode has baseline security standards or "best practices" that include employee training. As required by the 9/11 Act, security-related training programs for front-line employees in several modes will be implemented through the Federal regulatory process.

The sector's owners and operators have built a strong training and education foundation that includes a wide range of programs to effectively secure transportation assets, systems, and networks. For example, the sector is implementing a cross-modal exercise program with transit, rail, maritime, and highway partners. I-STEP engages modal partners to develop specific objectives and capabilities for its exercises with standardized performance measures.

Training, drills, and exercises may be funded through grant projects for intercity bus companies, mass transit systems (including intra-city bus, all forms of passenger rail, and ferry), and freight rail carriers consistent with legislative authorities. Furthermore, grant funds are provided to a single grantee to provide training resources for the trucking community. These activities have increased baseline awareness levels for employees and riders. Training and education initiatives are designed to reduce risks by enhancing deterrence, detection, prevention, resiliency, and response awareness.

8.3.5 Compliance and Assessment Processes

Compliance inspections and assessments are part of the data-gathering processes that support the risk management process. Compliance inspections are conducted to enforce regulatory requirements and standard security programs and to determine the effectiveness of voluntary standards, such as Security Action Items (SAIs) or best practices. Federal and State agencies have field inspectors who perform a variety of types of compliance inspections. Assessments are conducted to determine threats, vulnerabilities, or consequences associated with various threat scenarios. These assessments include Corporate Security Reviews, site-assistance visits, and audits. The 9/11 Act regulations will require vulnerability assessments and security plans for freight rail, public transportation, passenger rail, and over-the-road bus operators.

In some cases, findings of non-compliance are submitted for civil penalty processing. Other compliance audits provide valuable information about the effectiveness of protection and resiliency programs. The SSAs are developing a risk database to store pertinent data elements from compliance information, not traceable to the owner or operator, for the purpose of evaluating risks and the effectiveness of risk-reduction programs in and across the modes. It is envisioned the database will support strategic and operational assessments required under Federal statutes.

8.3.6 Intermodal Protection Process

Intermodal protection concerns arise at the interfaces between modes. Mass transit terminals, road and rail bridges across waterways, and port terminals are examples of infrastructure where several types of transportation conveyances converge. Storage yards, warehouses, and transfer points are way points in transportation where passengers or cargo shift from one mode to another. Protection of intermodal assets where several modal operations converge is handled through the risk management process as each mode identifies and assesses its critical infrastructure. Additionally, points in the supply chain where cargo is transferred from one mode to another should be considered for criticality assessments. In this latter context, intermodal protection is an aspect of security of the supply chain. The following examples list some mechanisms in the sector that address intermodal and supply chain protection:

- TSSRA
- VIPR
- I-STEP
- CCSP
- National Explosives Detection Canine Team Program
- R&DWG
- Critical Infrastructure Identification Process
- Container Seals Program
- Chemical Facility Anti-Terrorism Standards
- Customs-Trade Partnership Against Terrorism (C-TPAT)
- HAZMAT endorsements to Commercial Driver's Licenses (CDLs)

8.3.7 Response and Recovery

Response and recovery responsibilities of the sector are primarily managed by DOT in accordance with the NRF. DOT published the *National Transportation Recovery Strategy (NTRS)*¹⁴ in October 2009, to help transportation industry stakeholders and State, local, and tribal government officials prepare for and manage the transportation recovery process following a major disaster. The Federal agencies responsible for supporting response and recovery operations participate in Emergency Support Functions 1 and 7 of the NRF during a declared emergency.

8.3.8 Lessons-Learned Process

The SSAs have several processes for collecting lessons-learned information. TSA's I-STEP program collects exercise-related lessons learned which are then used by the private sector participants and by modal managers. The lessons learned are stored in the Exercise Information System (EXIS) database. The Coast Guard Standard After-action and Lessons-learned System (CG-SAILS) captures lessons-learned from operations, responses, and exercises.

Event-specific lessons learned are included in post-event reports from field and headquarters elements involved in response and recovery activities. These reports are distributed to responsible offices for action. Lessons learned that have applicability beyond the SSAs are submitted for posting in the Lessons-Learned Information Sharing (LLIS) system maintained by DHS. In addition, they are the basis for updating best practices, SAIs, and voluntary standards, and they inform the development of regulations, Emergency Amendments, and Security Directives.

8.4 Information Sharing and Protection

The sharing of relevant information regarding critical assets, systems, and networks among members of Federal, State, local, territorial, and tribal governments, and owners and operators is a key aspect of the sector's risk management framework. The TSISP describes the process for sharing critical intelligence and information throughout the sector. The TSISP reflects a vertical and horizontal network of communications for timely distribution of accurate and pertinent information. This TSISP incorporates requirements of legislation and the National Strategy for Information Sharing, dated October 31, 2007, and aligns with the Information Sharing Environment Implementation Plan (ISE-IP),¹⁵ dated November 2006.

¹⁴ https://www.dot.gov/disaster_recovery/resources/DOT_NTRS.pdf.

¹⁵ <http://www.fas.org/irp/agency/ise/plan1106.pdf>.

While the sector's GCC and SCC framework is an effective way for government and private sector representatives to coordinate efforts, additional mechanisms are available that foster more effective, efficient, and protected channels of communication and information sharing. The sector uses several federally-maintained platforms to share both classified and unclassified information, as indicated in the list below. Additional platforms exist to augment the emergency response agencies of the State, local, and tribal governments.

- Joint Worldwide Intelligence Communications System (JWICS)
- INTELINK Homeland Secure Data Network (HSDN)
- Secret Internet Protocol Router Network (SIPRNet)
- Non-secure Internet Protocol Router Network (NIPRNet)
- TSA Remote Access to Classified Enclaves (TRACE)
- TSA Automated Inspections, Enforcement, and Incident Reporting Subsystem
- Fusion Centers (Federal and State)
- Joint Terrorism Task Forces (JTTFs)

The sector's partners have a robust network of communications to exchange information. In order to facilitate multi-directional information flow between public and private sector partners, the SSA established a Transportation Security ISAC for the sector that integrates with Public Transportation, Rail, and Highway ISACs. Several other information-sharing mechanisms are currently used to facilitate coordination and collaboration. These include:

- GCCs and SCCs
- Homeland Security Information Network (HSIN)
- Lessons-Learned Information Sharing (LLIS)
- Homeland Security Advisory System (HSAS)
- Information Sharing and Analysis Centers (ISACs)
- Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)
- National Infrastructure Coordination Center (NICC)
- Transportation Security Operations Center (TSOC)
- Homeport
- Area Maritime Security Committees (AMSCs)
- Federal Register Notices

The sector also uses several communication and coordination mechanisms to exchange information on its cybersecurity initiatives, including:

- Cross-Sector Cyber Security Working Group (CSCSWG)
- Transportation Systems Sector Cyber Working Group (TSS CWG)
- Information Sharing and Analysis Centers (ISACs)



Appendix 1: Acronym List

The acronyms and abbreviations referenced in the base document of the 2010 Transportation Systems SSP are defined below:

9/11 Act	Implementing Recommendations of the 9/11 Commission Act of 2007
AAR	Association of American Railroads
AASHTO	American Association of State and Highway Transportation Officials
ACE	Automated Commercial Environment
ACI	Advance Commercial Information
AGA	American Gas Association
AGCC	Aviation Government Coordinating Council
AIP	Aviation Improvement Program
AIS	Automatic Identification System
ALERTS	Allied Law Enforcement for Rail and Transit Security
AMBER	America's Missing: Broadcast Emergency Response
AMRA	Aviation Modal Risk Assessment
AMSC	Area Maritime Security Committee
AMSP	Area Maritime Security Plan
Amtrak	The National Railroad Passenger Corporation
AN	Ammonium nitrate
ANS	Air Navigation Services
AOC	Airport Operating Certificate
AOPL	American Association of Pipe Lines
AOSSP	Aircraft Operator Standard Security Program
APEC	Asia Pacific Economic Cooperation
APGA	American Public Gas Association
API	American Petroleum Institute
APTA	American Public Transportation Association

ASAC	Aviation Security Advisory Committee
ASCC	Aviation Sector Coordinating Council
ASP	Airport Security Programs
AT	Advanced Technology
ATC	Air traffic control
ATCCRP	Advanced Tank Car Collaborative Research Program
ATSA	Aviation Transportation Security Act of 2001
BASE	Baseline Assessment for Security Enhancement
CAPTA	Costing Asset Protection: A Guide for Transportation Agencies
CARVER	Criticality, Accessibility, Recoverability, Vulnerability, Effect and Recognizability
CBP	U.S. Customs and Border Protection (DHS)
CBSA	Canadian Border Services Agency
CBRNE	Chemical, biological, radiological, nuclear, and explosive
CCSF	Certified Cargo Screening Facility
CCSP	Certified Cargo Screening Program
CFR	Code of Federal Regulations
CG-SAILS	Coast Guard Standard After-action and Lessons-learned System
CHEMTREC	Chemical Transportation Emergency Center
CIKR	Critical infrastructure and key resources
CIPAC	Critical Infrastructure Protection Advisory Council
COE	Centers of Excellence
COTP	Captain of the Port
CSAC	Chemical Security Analysis Center (DHS S&T)
CSCSWG	Cross-Sector Cyber Security Working Group
CSI	Container Security Initiative
CSR	Corporate Security Review
C-TPAT	Customs-Trade Partnership Against Terrorism
DASSP	Ronald Reagan Washington National Airport Access Standard Security Programs
DHS	U.S. Department of Homeland Security
DOC	U.S. Department of Commerce
DoD	U.S. Department of Defense
DOE	U.S. Department of Energy
DOJ	U.S. Department of Justice
DOS	U.S. Department of State
DOT	U.S. Department of Transportation

EA	Emergency Amendment
EEZ	Exclusive Economic Zone
EU	European Union
EXIS	Exercise Information System
FAA	Federal Aviation Administration
FAAP	Foreign Airport Assessment Program
FACA	Federal Advisory Committee Act
FAM	Federal Air Marshal
FAMS	Federal Air Marshal Service
FAMSAC	Federal Air Marshal Supervisory Agent in Charge
FAST	Free and Secure Trade
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FERC	Federal Energy Regulatory Commission
FFDO	Federal Flight Deck Officer
FHWA	Federal Highway Administration (DOT)
FMCSA	Federal Motor Carrier Safety Administration (DOT)
FMSC	Federal Maritime Security Coordinator
FOUO	For Official Use Only
FRA	Federal Railroad Administration (DOT)
FRSGP	Freight Rail Security Grant Program
FRZ	Flight restricted zone
FSMP	Facility Security Management Program
FTA	Federal Transit Administration (DOT)
FY	Fiscal year
G8	Group of Eight
GA	General aviation
GCC	Government Coordinating Council
GIS	Geographic Information System
GPS	Global Positioning System
HAZMAT	Hazardous materials
HEIED	Hand-emplaced improvised explosive device
HHS	U.S. Department of Health and Human Services
HITRAC	Homeland Infrastructure Threat and Risk Analysis Center (DHS)
HMC	Highway Infrastructure and Motor Carrier

HSA	Homeland Security Act of 2002
HSDN	Homeland Secure Data Network
HSIN	Homeland Security Information Network
HSIN-CS	Homeland Security Information Network-Critical Sectors
HSPD-5	Homeland Security Presidential Directive 5, Management of Domestic Incidents
HSPD-7	Homeland Security Presidential Directive 7, Critical Infrastructure Identification, Prioritization, and Protection
HSSM	Highway security-sensitive materials
HTUA	High-Threat Urban Area
IAC	Indirect Air Carrier
IBSGP	Intercity Bus Security Grant Program
IC	Intelligence Community
ICAO	International Civil Aviation Organization
ICS	Incident Command System
IDW	Infrastructure Data Warehouse
IED	Improvised explosive device
INGAA	Interstate Natural Gas Association of America
IP	Office of Infrastructure Protection (DHS)
IPT	Integrated Product Team
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
ISAC	Information Sharing and Analysis Center
ISE-IP	Information Sharing Environment Implementation Plan
ISPR	International Security Peer Review
ISPS	International Ship and Port Facility Security
I-STEP	Intermodal Security Training and Exercise Program
IT	Information technology
ITCC	Interagency Threat Coordination Committee
JTTF	Joint Terrorism Task Force
JWICS	Joint Worldwide Intelligence Communications System
LEOFA	Law Enforcement Officer Flying Armed
LES	Law Enforcement Sensitive
LLIS	Lessons Learned Information Sharing
LNG	Liquefied natural gas
LORAN	Long Range Navigation
LRIT	Long Range Identification and Tracking

MARAD	Maritime Administration
MARSEC	Maritime Security
MASSRA	Mission, Asset, and System Specific Risk Assessments
MD-3	Maryland Three Rule
MDA	Maritime Domain Awareness
MOU	Memorandum of Understanding
MPO	Metropolitan Planning Organization
MSRAM	Maritime Security Risk Analysis Model
MTS	Maritime Transportation System
MTSA	Maritime Transportation Security Act of 2002
NAR	National Annual Report
NAS	National Airspace System
NBTA	National Bus Traffic Association
NCIP R&D	National Critical Infrastructure Protection Research and Development
NCR	National Capital Region
NCSD	National Cyber Security Division (DHS)
NECD	Non-explosive cutting device
NEDCTP	National Explosives Detection Canine Team Program
NHS	National Highway System
NICC	National Infrastructure Coordination Center
NIPP	National Infrastructure Protection Plan
NIPRNet	Non-secure Internet Protocol Router Network
NIMS	National Incident Management System
NIST	National Institute of Standards and Technology (DOC)
NOAA	National Oceanic and Atmospheric Administration (DOC)
NOC	National Operations Center
NPRM	Notice of Proposed Rulemaking
NPRN	National Port Readiness Network
NRF	National Response Framework
NSPD-47	National Security Presidential Directive 47
NSSE	National Security Special Event
NSTS	National Strategy for Transportation Security
NSWC	Naval Surface Warfare Center
OGS	TSA Office of Global Strategies
OI	TSA Office of Intelligence

OLE	TSA Office of Law Enforcement
ONG	Oil and Natural Gas
OST	Operation Secure Transport
OSTP	Office of Science and Technology Policy
PAG	Peer Advisory Group
PCII	Protected Critical Infrastructure Information
PCIS	Partnership for Critical Infrastructure Security
PHMSA	Pipeline Hazardous Materials Safety Administration (DOT)
PIH	Poison inhalation hazard
PIP	Partners in Protection
POD	Partnership and Outreach Division (DHS IP)
PortSTEP	Port Security Training and Exercise Program
PSA	Protective Security Advisors (DHS)
PSS	Principal Security Specialist
PT-ISAC	Public Transit - Information Sharing and Analysis Center
R&D	Research and Development
R&DWG	Research and Development Working Group
RAN	Railroad Alert Network
RCA	Rail Corridor Assessment
RDT&E	Research, Development, Test, and Evaluation
RITA	Research and Innovative Technologies Administration
RMA	Risk Mitigation Activity
RSC	Rail Security Coordinator
RSRA	Rail Security Risk Assessment
RSSM	Rail security-sensitive material
S&T	Science and Technology Directorate (DHS)
SAFETEA-LU	Safe, Affordable, Flexible, Efficient Transportation Equity Act – A Legacy for Users
SAI	Security Action Item
SAR	Sector Annual Report
SBU	Sensitive But Unclassified
SCADA	Supervisory Control and Data Acquisition
SCC	Sector Coordinating Council
SD	Security Directive
Sector	Transportation Systems Sector
SIPRNet	Secret Internet Protocol Router Network

SPM	Sector Partnership Model
SSA	Sector-Specific Agency
SSA EMO	SSA Executive Management Office (DHS IP)
SSI	Sensitive Security Information
SSOA	State Safety Oversight Agency
SSP	Sector-Specific Plan
ST-ISAC	Surface Transportation Information Sharing and Analysis Center
STORMCAP	Security Training, Operational Readiness, and Maritime Community Awareness Program
STRAHNET	Strategic Highway Network
STSA	School Transportation Security Awareness
STSIP	Surface Transportation Security Inspection Program
TARR	Terrorist Activity Recognition and Reaction
TIH	Toxic inhalation hazard
TMC	Traffic Management Center
TRACE	TSA Remote Access to Classified Enclaves
TRB	Transportation Research Board
TSA	Transportation Security Administration
TSGP	Transit Security Grant Program
TSI	Transportation Security Incident
TSIR	Transportation Security Incident Report
TSI-S	Transportation Security Inspector – Surface (Surface Inspector)
TSISP	Transportation Security Information Sharing Plan
TSNM	TSA Office of Transportation Sector Network Management
TSO	Transportation Security Officer
TSOC	Transportation Security Operations Center
TSP	Trucking Security Program
TSS CWG	Transportation Systems Sector Cyber Working Group
TSSRA	Transportation Sector Security Risk Analysis
TTAC	TSA Office of Transportation Threat Assessment and Credentialing
TVC	Threat, Vulnerability, and Consequence
TWIC	Transportation Worker Identification Credential
USACE	U.S. Army Corp of Engineers
US-CERT	U.S. Computer Emergency Readiness Team
USCG	U.S. Coast Guard
USSS	U.S. Secret Service

VBIED	Vehicle-borne improvised explosive devices
VIPR	Visible Intermodal Prevention and Response
WMD	Weapon of Mass Destruction

Appendix 2: Glossary of Terms

Many of the definitions in this Glossary are derived from language enacted in Federal laws and/or included in national plans, including the Homeland Security Act (HSA) of 2002, the USA PATRIOT Act of 2001, the National Incident Management System (NIMS), the National Response Framework (NRF), and the 2009 National Infrastructure Protection Plan (NIPP).

All Hazards. A grouping classification encompassing all conditions, environmental or manmade, have the potential to cause injury, illness, or death; damage to or loss of equipment, infrastructure services, or property; or alternatively causing functional degradation to social, economic, or environmental aspects.

Asset. See Critical Infrastructure and Key Resources.

Capability Gap. Identified weakness in security posture.

Consequence. The effect of an event, incident, or occurrence. For the purposes of the 2009 NIPP, consequences are divided into four main categories: public health and safety, economic, psychological, and governance impacts.

Control Systems. Computer-based systems used within many infrastructure and industries to monitor and control sensitive processes and physical functions. These systems typically collect measurement and operational data from the field, process and display the information, and relay control commands to local or remote equipment or human-machine interfaces (operators). Examples of types of control systems include supervisory control and data acquisition (SCADA) systems, process control systems, and distributed control systems.

Critical Infrastructure and Key Resources (CIKR). Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any Federal, State, regional, local, tribal, or territorial jurisdiction. As defined in the HSA, key resources are publicly or privately controlled resources essential to the minimal operations of the economy and government.

Critical Infrastructure Partnership Advisory Council (CIPAC). Advisory council to the Secretary of Homeland Security providing the legal construct for collaborative engagement with the private sector as required by law and presidential directives.

Cybersecurity. The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability. Includes protection and restoration, when needed, of information networks and wire line, wireless, satellite, public safety answering points, and 911 communications systems and control systems.

Dependency. Dependencies are considered to be those relationships that, if interrupted, could significantly impact the performance of the transportation system and its overall resilience and those that could expose the public to serious health and safety risks or harm the economy.

Enabling Homeland Capabilities. The suite of technologies needed to close a capability gap.

Function. Service, process, capability, or operation performed by an asset, system, network, or organization.

Government Coordinating Council (GCC). The government counterpart to the SCC for each sector established to enable inter-agency coordination. The sector-wide GCC is composed of Federal, State, and local governments, and tribal representatives, and may identify gaps in plans, programs, policies, procedures, and strategies, and serve as the forum to work with the private sector to develop security and resiliency objectives, policies, and plans.

Interdependency. Interdependency covers a wide range of interconnected assets, physical and cyber, shared between multiple transportation assets, systems, and networks. The degree of interdependency does not need to be equal in both directions.

Key Resource. See Critical Infrastructure and Key Resources.

Level 1. Those facilities and systems that if successfully destroyed or disrupted through terrorist attack would cause major national or regional impacts similar to those experienced with Hurricane Katrina or the attacks of September 11, 2001.

Level 2. Those facilities and systems that meet predefined, sector-specific criteria and are not Level 1 facilities or systems.

Mitigation. Ongoing and sustained action to reduce the probability of, or lessen the impact of, an adverse incident. Mitigation measures may be implemented prior to, during, or after an incident and are often developed in accordance with lessons learned from prior incidents. Mitigation involves ongoing actions to reduce exposure to, probability of, or potential loss from hazards.

Modal Annex. Modal protection implementation plans that detail the individual characteristics of the mode and explain how each mode will apply risk management to protect its systems, assets, people, and goods.

Mode. One of six interconnected subsectors of the Transportation Systems Sector. They include: aviation, freight rail, highway and motor carrier, maritime, mass transit and passenger rail, and pipeline.

Network. A group of components that share information or interact with each other in order to perform a function.

Node. A network intersection or junction (e.g., a subway station).

Owners/Operators. Those entities responsible for day-to-day operation and investment in a particular asset or system.

Preparedness. Activities necessary to build, sustain, and improve readiness capabilities to prevent, protect against, respond to, and recover from natural or manmade incidents. Preparedness is a continuous process involving efforts among all levels of government, the private sector, and nongovernmental organizations to identify threats, determine vulnerabilities, and identify and provide resources to prevent, respond to, and recover from major incidents.

Prevention. Actions taken and measures put in place for the continual assessment and readiness of necessary actions to reduce the risk of threats and vulnerabilities, to intervene and stop an occurrence, or to mitigate effects.

Protected Critical Infrastructure Information (PCII). PCII refers to all critical infrastructure information, including categorical inclusion PCII, that has undergone the validation process and that the PCII Program Office has determined qualifies for protection under the Critical Infrastructure Information Act of 2002 (CII Act). All information submitted to the PCII Program Office or designee with an express statement is presumed to be PCII until the PCII Program Office determines otherwise.

Protection. Actions or measures taken to cover or shield from exposure, injury, or destruction. In the context of the SSP, protection includes actions to deter the threat, mitigate the vulnerabilities, or minimize the consequences associated with a terrorist attack or other incident. Protection can include a wide range of activities, such as hardening facilities, building resiliency and redundancy, incorporating threat resistance into initial facility design, initiating active or passive countermeasures, installing security systems, promoting workforce surety, training and exercises, and implementing cybersecurity measures, among various others.

Resilience. The National Infrastructure Advisory Council (NIAC) working definition of resilience describes infrastructure resilience as the ability to reduce the magnitude and/or duration of disruptive events. In the context of the Transportation

Systems Sector, resilience is the sector's ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions.

Risk. The potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.

Risk Management Framework. A planning methodology that outlines the process for setting goals and objectives; identifying assets, systems, and networks; assessing risks; prioritizing and implementing protection programs and resiliency strategies; measuring performance; and taking corrective action. Public and private sector entities often include risk management frameworks in their business continuity plans.

Sector. The NIPP addresses 18 CIKR sectors, identified by the criteria set forth in HSPD-7. The Transportation Systems Sector is a logical collection of assets, systems, and networks that transports people, food, water, medicines, fuel, and other commodities vital to the public health, safety, security, and economic well-being of our Nation. The Transportation Systems Sector (the sector) is comprised of six key, interconnected subsectors or modes (aviation, freight rail, highway and motor carrier, maritime, mass transit and passenger rail, and pipeline).

Sector Coordinating Council. The private sector counterparts to the GCC, these councils are self-organized, self-run, and self-governed organizations that are representative of a spectrum of key sector partners. SCCs serve as the government's principal point of entry into each sector for developing and coordinating a wide range of CIKR protection activities and issues.

Sector Partnership Model (SPM). The framework used to promote and facilitate sector and cross-sector planning, coordination, collaboration, and information sharing for CIKR protection involving all levels of government and private sector entities.

Sector-Specific Agency (SSA). Federal departments and agencies identified in HSPD-7 as responsible for CIKR protection activities in specified CIKR sectors.

Sector-Specific Plan (SSP). Augmenting plans that complement and extend the NIPP and detail the application of the NIPP framework specific to each of the 18 CIKR sectors. SSPs are developed by the SSAs in close collaboration with other sector partners.

Sensitive Security Information (SSI). Control designation used by DHS and applied to information such as security programs, vulnerability and threat assessments, screening processes, technical specifications of certain screening equipment and objects used to test screening equipment, and equipment used for communicating security information relating to air, land, or maritime transportation. SSI protects information that, if disclosed, would be an unwarranted invasion of personal privacy, reveal a trade secret or privileged or confidential commercial or financial information, or make it easier for hostile elements to avoid security controls. The applicable information is spelled out in greater detail in 49 CFR 1520.7.

System. Any combination of facilities, equipment, personnel, procedures, and communications integrated for a specific purpose.

Threat. An individual, entity, or action that has the potential to deliberately harm life and/or property.

Value Proposition. A statement that outlines the national and homeland security interest in protecting the Nation's CIKR and articulates the benefits gained by all CIKR partners through the risk management framework and public-private partnership described in the NIPP.

Vulnerability. A physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.



Appendix 3: Transportation Systems Sector Authorities

Aviation & Transportation Security Act of 2001 (ATSA) established the Transportation Security Administration (TSA) within the Department of Transportation (DOT). TSA's three major mandates were to: take responsibility for security for all modes of transportation; recruit, assess, hire, train, and deploy Security Officers for 450 commercial airports from Guam to Alaska in 12 months; and provide 100 percent screening of all checked baggage for explosives by December 31, 2002.

In March 2003, TSA transitioned from DOT to the Department of Homeland Security (DHS), which was created on November 25, 2002 by the Homeland Security Act (HSA) of 2002, unifying the Nation's response to threats to the homeland.

Executive Order 10173: Prescribing Regulations Relating to the Safeguarding of Vessels, Harbors, Ports, and Waterfront Facilities of the United States, as amended by subsequent Executive Orders, promulgates implementation authority for port security activities in the form of regulations at 33 CFR 6 under the discretionary authority of the Magnuson Act of 1950. 33 CFR 6 remains one of the principal authorities that is available to each Coast Guard Captain of the Port (COTP) for port security and provides authority that can be used to rectify non-compliance with 33 CFR 101 et. seq.

Executive Order 12656: Assignment of Emergency Preparedness Responsibilities, issued under various authorities, includes requirements for development of plans and procedures for maritime and port safety, law enforcement and security, and for emergency operation of U.S. ports and facilities.

Executive Order 13416: Strengthening Surface Transportation Security builds upon the improvements made in surface transportation security since the attacks of September 11, 2001, specifically actions taken under HSPD-7. Executive Order 13416 requires the strengthening of the U.S. surface transportation systems by facilitating and implementing a comprehensive, coordinated, and efficient security program. The order sets deadlines for key security activities including security assessments of each surface transportation mode and an evaluation of the effectiveness and efficiency of current Federal Government surface transportation security initiatives.

Homeland Security Act of 2002 (HSA) established DHS under a broad mandate. The primary mission of DHS is to prevent terrorist attacks within the United States. DHS is tasked to reduce the vulnerability of the United States to terrorism, and to minimize the damage, and assist in the recovery, from terrorist attacks that do occur within the United States. As detailed in the HSA, these objectives are to be accomplished through coordination with non-Federal entities including State, local, and tribal government officials, as well as a wide range of private sector partners.

The HSA established TSA as a distinct entity within DHS under the Under Secretary for Border and Transportation Security. Aviation security has been a major focus of TSA and its functions include deploying explosive detection systems at airports and screening checked baggage for hazardous materials. Following the Administration's creation, TSA enacted the Secure Flight Program in 2002. Under this Program, TSA receives passenger and certain non-traveler information, conducts watch list

matching against the No-Fly and Selectee portions of the Federal Government's consolidated terrorist watch list, and transmits a boarding pass printing result back to aircraft operators.

Homeland Security Presidential Directive 5: Management of Domestic Incidents (HSPD-5) establishes a national approach to domestic incident management that ensures effective coordination among all levels of government and between the government and the private sector. Central to this approach is the NIMS, an organizational framework for all levels of government, and the NRF, an operational framework for national incident response.

In this directive, the President designates the Secretary of Homeland Security as the principal Federal official for domestic incident management and empowers the Secretary to coordinate Federal resources used for prevention, preparedness, response, and recovery related to terrorist attacks, major disasters, or other emergencies. The directive assigns specific responsibilities to the Attorney General, Secretary of Defense, Secretary of State, and the Assistants to the President for Homeland Security and National Security Affairs, and directs the heads of all Federal departments and agencies to provide their "full and prompt cooperation, resources, and support," as appropriate and consistent with their own responsibilities for protecting national security, to the Secretary of Homeland Security, Attorney General, Secretary of Defense, and Secretary of State in the exercise of leadership responsibilities and missions assigned in HSPD-5.

Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection (HSPD-7) establishes a national policy for Federal departments and agencies to identify and prioritize critical infrastructure and to protect them from terrorist attacks. Federal departments and agencies work with State and local governments, and the private sector to accomplish this objective. Consistent with this directive, the Secretary of Homeland Security identifies, prioritizes, and coordinates the protection of CIKR with an emphasis on those that could be exploited to cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction. The Secretary establishes uniform policies, approaches, guidelines, and methodologies for integrating Federal infrastructure protection and risk management activities within and across sectors along with metrics and criteria for related programs and activities.

The Transportation Systems Sector plays an important role in carrying out HSPD-7 by pursuing a layered approach to security and using risk analysis to guide decisionmaking. The SSAs identify areas of high risk and set baseline security standards to create measurable risk reduction targets.

Homeland Security Presidential Directive 8: National Preparedness (HSPD-8) is a companion directive HSPD-5, establishing policies and outlining actions that strengthen the U.S. preparedness capabilities of Federal, State, and local entities in order to prevent or respond to threatened or actual national domestic terrorist attacks, major disasters, or other emergencies. HSPD-8 requires a national domestic all-hazards preparedness goal, with established mechanisms for improved delivery of Federal preparedness assistance to State and local entities.

Homeland Security Presidential Directive 9: Defense of United States Agriculture and Food (HSPD-9) establishes national policy to defend the agriculture and food system against terrorist attacks, disasters, and other emergencies. TSA has participated in a number of meetings and focus/working groups with the U.S. Department of Agriculture (USDA) and the Food and Drug Administration (FDA) to increase cooperation on security and protection efforts for food/agricultural product transportation.

Homeland Security Presidential Directive 13: Maritime Security Policy (HSPD-13) establishes U.S. policy, guidelines, and implementation actions to enhance U.S. national security and homeland security by protecting U.S. maritime interests. It directs the coordination of U.S. Government maritime security programs and initiatives to achieve a comprehensive and cohesive national effort involving appropriate Federal, State, local, and private sector entities. This directive also establishes a Maritime Security Policy Coordinating Committee to coordinate interagency maritime security policy efforts.

The objective of HSPD-13 is to prevent terrorist attacks, criminal acts, or hostile acts in, or the unlawful exploitation of, the Maritime Domain, and reducing the vulnerability of the Maritime Domain to such acts and exploitation. It seeks to enhance U.S. national security and homeland security by protecting U.S. population centers, critical infrastructure, borders, harbors,

ports, and coastal approaches. HSPD-13 aims to maximize recovery and response from attacks within the Maritime Domain, and maximizing awareness of security issues in the Maritime Domain in order to support U.S. forces and improve U.S. Government actions in response to identified threats.

Homeland Security Presidential Directive 16: Aviation Security Policy (HSPD-16) provides a strategic vision for aviation security and directs the production of a National Strategy for Aviation Security and supporting plans. The supporting plans address the following areas:

- Aviation transportation system security;
- Aviation operational threat response;
- Aviation transportation system recovery;
- Air domain surveillance and intelligence integration;
- Domestic outreach; and
- International outreach.

Aviation Security Policy aims to deter and prevent terrorist attacks and criminal or hostile acts in the Air Domain and protect the United States and its interests in the Air Domain. It seeks to increase resiliency and mitigate damage, expedite recovery, and minimize the impact on the Aviation Transportation System and the U.S. economy in the case of an incident.

In accordance with NSPD-47/HSPD-16, the Secretary of Homeland Security is responsible for closely coordinating U.S. Government activities encompassing the national aviation security programs including identifying conflicting procedures, identifying vulnerabilities and consequences, and coordinating corresponding interagency solutions. The Secretary must also actively engage domestic and international partners to facilitate coordination and communication.

Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act) includes multiple requirements and recommendations dealing with transportation security. The 9/11 Act recommends that the U.S. government identify and evaluate the transportation assets that need to be protected, and set risk-based priorities for defending them. Decisionmakers are to select the most practical and cost effective ways of doing so, and then develop plans, budgets, and funding to implement the efforts. The 9/11 Act authorizes funding levels for various efforts of TSA, including \$1.99 billion for railroad security, \$95 million for over-the-road bus and trucking security, and \$36 million for hazardous material and pipeline security through fiscal year 2011.

The 9/11 Act establishes a TSISP in consultation with the Program Manager of the Information Sharing Environment, the Secretary of Transportation, and public and private sector partners. The 9/11 Act requires that, within three years of passage, the Secretary of Homeland Security establish a system that screens 100 percent of cargo transported on passenger aircraft. It also requires all maritime cargo to be scanned by non-obtrusive imaging equipment by July 1, 2012, and allows the Secretary to extend the deadline by two year increments if certain benchmarks are not met.

Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) defines the requirements for the National Strategy for Transportation Security (NSTS). The NSTS includes an identification and evaluation of the transportation assets in the U.S. that, in the interests of national security and commerce, must be protected from attack or disruption by terrorist or other hostile forces. The sector must develop risk-based priorities across all transportation modes and establish realistic deadlines for addressing security needs in a cost-effective manner. Finally, the NSTS requires a forward-looking strategic plan that sets forth the agreed upon roles and missions of Federal, State, regional, and local authorities and establishes mechanisms for encouraging private sector cooperation and participation in the implementation of the plan.

The Western Hemisphere Travel Initiative (WHTI) is a result of the IRTPA, and requires all travelers to present a passport or other document that denotes identity and citizenship when entering the United States. The goal of WHTI is to strengthen

U.S. border security while facilitating entry for U.S. citizens and legitimate foreign visitors by providing standardized documentation that enables DHS to quickly and reliably identify a traveler.

Magnuson Act of 1950 (50 United States Codes (U.S.C.) 190 et. seq.) enables the President to institute rules and regulations pertaining to the anchorage and movement of foreign-flag vessels in U.S. territorial waters, to inspection, and, if necessary, securing of such vessels, and to guarding against sabotage, accidents, or other acts against vessels, harbors, ports, and waterfront facilities. It provides the basis for issuance of security zones and COTP orders to control vessel movement and security of waterfront facilities. It contains broad authority to create security zones or issue COTP orders to regulate vessels or waterfront facilities within the territorial sea.

National Maritime Transportation Security Act of 2002 (MTSA) provides a framework for ensuring the security of maritime commerce and our Nation's domestic ports. MTSA's key requirement is to prevent a Transportation Security Incident, which has been a core mission of the USCG since its inception, and it broadens the USCG's authorities in this area. It is complimentary to the International Ship and Port Facility Security Code. The USCG's International Port Security Program engages in bilateral and multilateral discussion with maritime trading nations worldwide in order to exchange information and share best practices regarding the implementation of the International Ship and Port Facility Security code and other international maritime security standards.

Ports and Waterways Safety Act (33 U.S.C. 1221 et seq.) provides USCG with broad basic authority for the creation of safety and security zones, regulated navigation areas, and COTP orders all of which can be used to control the movement of vessels as well as advance notice of arrival requirements for vessels. It also provides for the establishment, operation, and maintenance of vessel traffic services. In most instances, this authority applies within the territorial sea. In addition, 33 U.S.C. §1226 contains specific authority to prevent or respond to acts of terrorism against individuals, vessels, or public or commercial structures within or adjacent to the marine environment. The statute provides civil penalties for regulatory enforcement, facilitating administration of port safety measures. The statute, as amended, provides authority that supports port safety and security measures needed for Maritime Security regimes and regulations and Marine Transportation System recovery following an incident.

The Post-Katrina Emergency Reform Act of 2006, signed into law October 4, 2006, establishes new leadership positions within DHS and adds functions for FEMA to address catastrophic planning and preparedness. The Act creates and reallocates functions to other components within the Department, and amends the HSA, in ways that directly and indirectly affect the organization and functions of various entities within DHS.

DHS IP is designated to identify risks, threats, and vulnerabilities to critical infrastructure, and develop methods to mitigate them. IP will continue to help strengthen the first line of defense against attacks on the Nation's critical infrastructure and provide robust real-time monitoring and response to incidents of national significance. The DHS Office of Risk Management and Analysis, formerly within IP, will directly report to the Under Secretary and will expand its focus from physical critical infrastructure to cybersecurity and other risk analysis arenas. This expanded mission will broaden the Office's efforts to address risk issues for the overall protection, prevention, and mitigation of homeland security risks.

Security and Accountability for Every Port Act of 2006 (SAFE Port Act) is a comprehensive maritime and cargo security bill intended to strengthen port security across the Nation by establishing improved cargo screening standards, providing incentives to importers to enhance security measures, and implementing a framework to ensure the successful resumption of shipping in the event of a terrorist attack, while preserving the flow of commerce. The SAFE Port Act established programs such as TWIC, the Container Security Initiative, and the C-TPAT. In addition, the Act created the Domestic Nuclear Detection Office within DHS and appropriated funds toward the Integrated Deepwater System Program, a long-term USCG modernization program.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) is a broad mandate to enhance domestic security against terrorism. Government surveillance capabilities are increased, and a Counterterrorism Fund is established within the Treasury.

In addition to general counterterrorism measures, the USA PATRIOT Act includes transportation security-specific sections. It amends the Federal criminal code to prohibit specific terrorist acts or otherwise destructive, disruptive, or violent acts against mass transportation vehicles, ferries, providers, employees, passengers, or operating systems. It also amends the Federal transportation code to prohibit States from licensing any individual to operate a motor vehicle transporting hazardous material unless the Secretary of Transportation determines that such individual does not pose a security risk warranting denial of the license.



Appendix 4: Transportation Systems Sector Partners

Additional Security Partners

The Transportation Systems SSAs work collaboratively with numerous sector partners to ensure its security and the free flow of goods and passengers. Appendix 4 includes a list of additional sector partners that are not mentioned in the base plan of the SSP. However they play an important role in achieving the sector's protection and resiliency goals and objectives.

- **Department of Homeland Security (DHS)**

- **Office of Infrastructure Protection (IP).** DHS IP, now part of the National Protection and Programs Directorate (NPPD), has the overall responsibility for coordinating implementation of the NIPP across the 18 CIKR sectors; overseeing the development of 18 SSPs that outline processes and measures to secure the Nation's CIKR; providing training and plans for protective measures to assist owners and operators in securing the CIKR within their control; and helping State, local, tribal, territorial, and private sector partners develop the capabilities to mitigate vulnerabilities and identifiable risks to their assets. Through the NIPP sector partnership model, DHS IP coordinates security activities to reduce the Nation's vulnerabilities or to threats through a unified national approach.
- **Federal Protective Service.** As of October 2009, the Federal Protective Service is a Federal law enforcement component of NPPD that provides integrated security and law enforcement services to federally owned and leased buildings, facilities, properties, and other assets.
- **Federal Law Enforcement Training Center (FLETC).** FLETC provides basic and advanced training for Federal law enforcement agency personnel at DHS and the DOT. FLETC also provides training for State and local law enforcement officers and other security personnel.
- **Office of Intelligence and Analysis (I&A).** DHS I&A ensures that information is gathered from all relevant field operations and other parts of the Intelligence Community; is analyzed with a mission-oriented focus; is informative to senior decisionmakers; and is disseminated to the appropriate Federal, State, local, and private sector partners.
- **Homeland Infrastructure Threat and Risk Analysis Center (HITRAC).** HITRAC is the DHS infrastructure-intelligence fusion center that maintains situational awareness of infrastructure sectors and develops long-term strategic assessments of their risks by integrating threat information with the unique vulnerabilities and consequences of attack for each infrastructure sector.
- **Immigration and Customs Enforcement (ICE).** ICE is the largest DHS investigative bureau. ICE includes the investigative and intelligence resources of the former U.S. Customs Service, and the former Immigration and Naturalization Service, bringing together more than 20,000 employees who focus on enforcing immigration and customs laws within the United States and the protection of specified Federal buildings.

- **Science and Technology Directorate (S&T).** S&T is the primary research and development (R&D) arm of DHS. It provides Federal, State, and local officials with the technology and capabilities to protect the homeland, as well as managing the Transportation Security Laboratory.
- **Federal Emergency Management Agency (FEMA).** FEMA is responsible for providing training; securing funds to purchase equipment; providing support for planning and execution exercises; and offering technical assistance and other support to assist States and local jurisdictions to prevent, respond to, and recover from natural and manmade catastrophic events.
- **Department of Defense (DoD).** This list includes DoD-related agencies that support the Transportation Systems Sector in achieving its goals and objectives:
 - **North American Aerospace Defense Command (NORAD).** NORAD provides detection, validation, and warning of attacks against North America by aircraft, missiles, or space vehicles, and aerospace control of air-breathing threats to North America. NORAD obtains processes, assesses, and disseminates appropriate intelligence/information to provide timely warnings of maritime threats or attacks against North America.
 - **Office of Naval Intelligence (ONI).** ONI supports joint operational commanders with a worldwide organization and an integrated workforce of active duty, reserve, officer, enlisted, and civilian professionals. At the National Maritime Intelligence Center, ONI brings military and civilian employees into a single command to provide “one-stop shopping” for national-level maritime intelligence.
 - **Defense Joint Intelligence Operations Center (DJIOC).** DJIOC was established to integrate and synchronize military and national intelligence capabilities. DJIOC will plan, prepare, integrate, direct, synchronize, and manage continuous, full-spectrum Defense Intelligence Operations in support of the Combatant Commands. This will be a collaborative, interactive relationship with the Office of the Director of National Intelligence (ODNI), national intelligence agencies and centers, Combatant Command JIOCs, Combat Support Agencies, the Armed Services intelligence organizations, and the Joint Functional Component Command for Intelligence, Surveillance, and Reconnaissance to create a system-of-systems JIOC enterprise network-enabled by enterprise information technology architecture.
 - **U.S. Army Corps of Engineers (USACE).** USACE is responsible for maintaining the Nation’s commercial waterways, including levees, and operating the dams and locks that facilitate commerce on inland waterways.
 - **U.S. Northern Command (USNORTHCOM).** USNORTHCOM conducts operations to deter, prevent, and defeat threats and aggression aimed at the United States and its Territories and interests within the assigned area of responsibility. As directed by the President or Secretary of Defense, it provides military assistance to civil authorities, including consequence management operations. USNORTHCOM’s area of responsibility includes air, land, and sea approaches and encompasses the continental U.S., Alaska, Canada, Mexico, and the surrounding water out to approximately 500 nautical miles. It also includes the Gulf of Mexico and the Straits of Florida.
 - **U.S. Pacific Command (USPACOM).** USPACOM conducts operations to deter, prevent, and defeat threats and aggression aimed at the United States and its Territories, and interests within the assigned area of responsibility. As directed by the President or Secretary of Defense, it provides military assistance to civil authorities, including consequence management operations. USPACOM’s area of responsibility encompasses Hawaii and U.S. Territories, possessions, and freely associated states in the Pacific.
 - **U.S. Transportation Command (USTRANSCOM).** USTRANSCOM provides air, land, and sea transportation for the Department of Defense, both in times of peace and times of war, in support of the President and Secretary of Defense, and Combatant Commander-assigned missions.
- **Department of Justice (DOJ).** DOJ acts to reduce criminal and terrorists threats, and investigates and prosecutes actual or attempted attacks on, sabotage of, or disruptions of CIKR in collaboration with DHS. DOJ investigates and prosecutes criminal offenses and represents the Federal Government in litigation. The major investigative agencies—the Federal Bureau

of Investigation (FBI), the Drug Enforcement Administration (DEA), and the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF)—prevent and deter crime and apprehend criminal suspects. DOJ contributes to the sector through its law enforcement role. In the national effort to identify, prevent, and prosecute terrorists within the sector, TSA works closely with the FBI, which maintains lead responsibility for investigations of terrorists' acts or threats by individuals or groups inside the United States where such acts are within the Federal criminal jurisdiction of the United States.

- **Department of Transportation (DOT)**

- **Federal Aviation Administration (FAA).** FAA is charged with safely and efficiently operating and maintaining the Nation's aviation system. The FAA's major roles include regulating civil aviation to promote safety; encouraging and developing civil aeronautics, including new aviation technology; developing and operating a system of air traffic control and navigation for both civil and military aircraft; researching and developing the National Airspace System; developing and conducting programs to control aircraft noise and other environmental effects of civil aviation; and regulating U.S. commercial space transportation.
- **Federal Highway Administration (FHWA).** FHWA is charged with the responsibility of ensuring that America's roads and highways continue to be the safest and most technologically up-to-date. Although State, local, and tribal governments own most of the Nation's highways, FHWA provides financial and technical support to them for constructing, improving, and preserving America's highway system through administration of the Federal Aid and Federal Lands Highway Programs.
- **Federal Motor Carrier Safety Administration (FMCSA).** The primary mission of the FMCSA is to reduce crashes, injuries, and fatalities involving large trucks and buses. FMCSA also has responsibility for overseeing safe and secure highway transportation of hazardous materials and compliance of household goods movements. FMCSA accomplishes its mission through a strong partnership with law enforcement in the United States.
- **Federal Railroad Administration (FRA).** FRA promulgates and enforces railroad safety regulations, administers railroad assistance programs, conducts research and development in support of improved railroad safety and national railroad transportation policy, provides for the rehabilitation of Northeast Corridor railroad passenger service, and consolidates government support of railroad transportation activities.
- **Federal Transit Administration (FTA).** As part of a continuous effort to secure our nation's transit infrastructure, FTA has undertaken an aggressive nationwide security program, receiving full cooperation and support from every transit agency. FTA has conducted risk and vulnerability assessments and deployed technical assistance teams to help strengthen security and emergency preparedness plans, and has funded emergency response drills conducted in conjunction with local fire, police, and emergency responders. FTA has also implemented programs to improve public transit focusing on three priorities: training all transit employees and supervisors, improving emergency preparedness, and increasing public awareness of security issues.
- **Maritime Administration (MARAD).** MARAD promotes development and maintenance of a Marine Transportation System (MTS) sufficient to move the Nation's waterborne commerce and capable of serving the deployment requirements of the DoD. It engages in outreach and coordination activities in order to assist the maritime industry in emergency preparedness and response and recovery efforts related to maritime transportation security incidents and natural disasters. The outreach and coordination activities include interaction with MTS stakeholders in planning and training forums, conferences, workshops, exercises, and real world response and recovery efforts. MARAD provides a range of MTS information and emergency coordination capabilities through its Gateway Offices, Division Offices and the Office of Emergency Preparedness. Disaster response and recovery missions closely parallel the Ready Reserve Force (RRF) military support mission. RRF ships have inherent capabilities to support response and recovery efforts including provision of storage for petroleum or potable water, large areas suitable for shelters or field-grade hospitals, electric power generation capability, emergency communications, dining facilities, command and control platforms and room to carry large equipment. These RRF ships are available in appropriate circumstances to aid in response and recovery efforts.

- **National Highway Traffic Safety Administration (NHTSA).** NHTSA's mission is to save lives, prevent injuries, and reduce economic costs due to road traffic crashes through education, research, safety standards, and enforcement activity. NHTSA also serves as the lead Federal agency for Emergency Medical Services coordination and houses the National 9-1-1 Implementation Coordination Office, which are vital to our preparedness and response to all hazards.
- **Office of Intelligence, Security, and Emergency Response (S-60).** S-60 serves as DOT's focal point for leadership and direction on intelligence and security matters, and executes the Secretary's delegated authorities for DOT emergency management. Further, S-60 has overall Department lead responsibility for development and implementation of all responsibilities under the NRF and NIPP. As DOT's leading office on transportation emergency management, S-60 directs DOT's overall prevention, preparedness, response, and recovery efforts, to include: providing support for the DOT Crisis Coordinator; providing transportation threat notifications; directing the intra- and inter-agency emergency coordination efforts at the regional level; developing and maintaining DOT's emergency management strategy, policies, and plans; and operating DOT's Crisis Management Center.
- **Pipeline and Hazardous Materials Safety Administration (PHMSA).** PHMSA oversees the safety of more than 1.2 million daily shipments of hazardous materials in the United States and 2.3 million miles of pipeline through which two-thirds of the Nation's energy supply is transported. PHMSA is dedicated solely to working toward the elimination of transportation-related deaths and injuries in hazardous materials and pipeline transportation, and by promoting transportation solutions that enhance the resilience of communities and protect the natural environment.
- **Research and Innovative Technologies Administration (RITA).** RITA coordinates DOT research programs and is charged with advancing the deployment of cross-cutting technologies to improve our Nation's transportation system. As directed by Congress in its founding legislation, RITA leads DOT in coordinating, facilitating, and reviewing the Department's R&D programs and activities; advancing innovative technologies, including intelligent transportation systems; performing comprehensive transportation statistics research, analysis, and reporting; and providing education and training in transportation and transportation-related fields.
- **Saint Lawrence Seaway Development Corporation (SLSDC).** SLSDC, a wholly-owned Government corporation and an operating administration of DOT, is responsible for the operations and maintenance of the U.S. portion of the St. Lawrence Seaway between Montreal and Lake Erie. This responsibility includes managing vessel traffic control in areas of the St. Lawrence River and Lake Ontario, as well as maintaining and operating the two U.S. Seaway locks located in Massena, NY. The SLSDC coordinates its activities with its Canadian counterpart, the St. Lawrence Seaway Management Corporation, to ensure that the U.S. portion of the St. Lawrence Seaway, including the two U.S. locks, are available for commercial transit during the navigation season (usually late March to late December of each year). Additionally, the SLSDC performs trade development activities designed to enhance the utilization of the Great Lakes St. Lawrence Seaway System.
- **Department of Agriculture (USDA).** USDA sets public policy to protect and secure the Nation's food supply, agricultural base, and natural resources. On January 30, 2004, Homeland Security Presidential Directive 9 (HSPD-9) established a national policy to defend the agriculture and food system against terrorist attacks, disasters, and other emergencies. The directive also fosters a cooperative working relationship among DHS, USDA, and the Department of Health and Human Services (HHS) in expanding and conducting vulnerability assessments, mitigation strategies, and response planning. Since there are key interdependencies between the sector and the Food and Agriculture Sector and its component agencies (USDA and the Food and Drug Administration), future planning efforts continue to consider integrating security and protective policies and initiatives where appropriate between the two sectors.
- **Department of State (DOS).** DOS conducts diplomacy, a mission based on the role of the Secretary of State as the President's principal foreign policy advisor. DOS leads representation of the United States overseas and advocates U.S. policies with foreign governments and international organizations. DOS plays an important role in coordinating transportation protection issues with foreign governments and addressing issues concerning the protection and security of pipelines that cross national

boundaries, transportation-related concerns over international waterways, and through the aviation, highway, and freight rail modes that transport goods and people across international boundaries daily.

- **Food and Drug Administration (FDA).** FDA is responsible for carrying out certain provisions of the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (PL107-188), specifically Subtitle A (Protection of Food Supply) and Subtitle B (Protection of Drug Supply) of Title III. On January 30, 2004, HSPD-9 was released, establishing a national policy to defend the agriculture and food system against terrorist attacks, disasters, and other emergencies. TSA has participated in a number of meetings and focus/working groups with USDA and FDA to increase cooperation on security and protection efforts for food/agricultural product transportation.
- **National Counterproliferation Center (NCPC).** NCPC coordinates strategic planning within the Intelligence Community (IC) to enhance intelligence support of U.S. efforts to stem the proliferation of weapons of mass destruction and related delivery systems. NCPC works with the IC to identify critical intelligence gaps or shortfalls in collection, analysis, or exploitation, and to develop solutions to ameliorate or close these gaps. It also works with the IC to identify long-term proliferation threats and requirements, and to develop strategies to ensure that the IC is positioned to address these threats and issues. NCPC reaches out to elements both inside and outside of the IC, and the Federal Government to identify new methods or technologies that can enhance the capabilities of the IC to detect and defeat future proliferation threats.
- **National Counterterrorism Center (NCTC).** NCTC serves as the primary organization in the Federal Government for integrating and analyzing all intelligence pertaining to terrorism and counterterrorism and conducting strategic operational planning by integrating all instruments of national power.
- **National Geospatial-Intelligence Agency (NGA).** NGA provides timely, relevant, and accurate geospatial intelligence (GEOINT) to support national security domestically and abroad. NGA's geospatial-intelligence products serve a variety of military, civil, and international needs. In terms of transportation security, GEOINT provides the fundamental properties of geographical location associated with the data critical to maintaining appropriate posture and awareness, and also provides the value-added analyses required to create a distinct type of actionable intelligence for time-sensitive transportation issues.
- **Surface Transportation Board (STB).** When STB determines that a shortage of equipment, traffic congestion, unauthorized cessation of operations, or other failures of traffic management exist that create an emergency situation of such magnitude as to have substantial adverse effects on shippers or on rail service in a region of the United States, or that a rail carrier cannot transport the traffic offered to it in a manner that properly serves the public, STB may, for up to 270 days, direct the handling, routing, and movement of the traffic of a rail carrier and its distribution over its own or other railroad lines, and give directions for preference or priority in the transportation of traffic.

Advisory Councils

- **American Association of State Highway and Transportation Officials (AASHTO) Special Committee on Transportation Security and Emergency Management (SCOTSEM).** SCOTSEM membership includes all modes of transportation. SCOTSEM is the focal point for those engaged in transportation security and emergency management in State-level DOT to interface with the Federal DOT and DHS/TSA partners and industry stakeholders to exchange ideas, inform each other, develop issues, and formulate research projects that result in resolving issues, reducing or eliminating gaps, and developing training material and tools necessary for implementing the results of research or lessons learned. SCOTSEM focuses on all threats and hazards and multi-threat and multi-hazard environments and issues.
- **Critical Infrastructure Partnership Advisory Council (CIPAC).** To secure our Nation's most critical infrastructure, the Federal Government and private sector collaborate to identify, prioritize, and coordinate CIKR protection, as well as share information about physical, human, and cyber threats, vulnerabilities, incidents, and potential protective measures and best practices. To facilitate the successful execution of the sector partnership model and to develop resilience and protection plans, members of the Sector Coordinating Councils and Government Coordinating Councils require an environment

where they can discuss sensitive security matters. DHS established CIPAC as an advisory council to the Secretary of Homeland Security under the provisions of the Homeland Security Act. CIPAC is exempt from the requirements of the Federal Advisory Committee Act (FACA). This is intended to enhance meaningful discussions between the Federal, State, and local governments and the private sector on critical infrastructure protection issues. The process facilitates the effective and efficient sharing of information and advice about sector strategies, protective programs and measures, threats, vulnerabilities, and best practices. GCC and SCC members must register to participate in CIPAC.

- **Aviation Security Advisory Committee (ASAC).** ASAC's mission is to examine areas of civil aviation security as tasked by TSA with the aim of developing recommendations for improving civil aviation security methods, equipment, and procedures.
- **Homeland Security Advisory Council (HSAC).** HSAC provides advice and recommendations to the Secretary of Homeland Security on matters related to homeland security. The council is comprised of leaders from State and local governments, first-responder communities, the private sector, and academia.
- **Marine Transportation System National Advisory Council (MTSNAC).** Sponsored by the Maritime Administration (MARAD), the MTSNAC comprises 30 sector partners throughout the MARAD Marine Transportation System (MTS) initiative. The council provides advice to the Secretary of Transportation on the state of the Nation's MTS and how it can meet the Nation's economic needs out to 2020. The Security Committee of the Council works closely with the USCG, TSA, CBP, and other sector partners to address issues of cargo, port, and container security.
- **National Infrastructure Advisory Council (NIAC).** NIAC is the President's principal advisory panel on critical infrastructure protection issues spanning all sectors. NIAC is composed of not more than 30 members, appointed by the President, who are selected from the private sector, academia, and State and local government, representing senior executive leadership expertise from the CIKR areas as delineated in HSPD-7. Issues addressed range from risk assessment and management to information sharing and protective strategies. NIAC provides the President, through the Secretary of Homeland Security, with advice on the security of physical and cyber critical infrastructure supporting important sectors of the economy. It also has the authority to provide advice directly to the heads of other departments that have shared responsibility for critical infrastructure protection, including DHS, DOT, and DOE. NIAC is charged with improving the cooperation and partnership between the public and private sectors in securing critical infrastructure and advises on policies and strategies that range from risk assessment and management to information sharing, protective strategies, and clarifying the roles and responsibilities between the public and private sectors.
- **National Maritime Security Advisory Committee (NMSAC).** NMSAC provides advice to the Secretary of Homeland Security via the Commandant of USCG on matters such as national security strategy and policy, actions required to meet current and future all hazard threats, international cooperation on protection and security issues, and the protection concerns of the maritime transportation industry.
- **National Port Readiness Network (NPRN).** NPRN is an organization of nine Federal agencies:
 - DOT MARAD (chair)
 - USCG
 - TSA
 - U.S. Army Corps of Engineers (USACE)
 - U.S. Transportation Command (USTRANSCOM)
 - U.S. Northern Command (USNORTHCOM)
 - Military Sealift Command
 - Surface Deployment and Distribution Command

- U.S. Army Forces Command
- U.S. Army Installation Management Command (MCOM)

These agencies' responsibilities include supporting the secure movement of military forces through U.S. ports. The organization includes a steering group, a working group, and local port readiness committees at 17 strategic commercial ports and provides coordination and cooperation to ensure the readiness of commercial ports and intermodal facilities to support deployment during contingencies and other defense emergencies.

- **National Institute of Standards and Technology (NIST).** NIST is a non-regulatory Federal agency within the Department of Commerce's (DOC) Technology Administration. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. NIST, the only Federal metrology institute, has developed numerous homeland security-related minimum performance standards, participates in several standards setting bodies related to homeland security, has extensive experience in designing and developing test and evaluation programs, provides nationally recognized accreditation of testing laboratories, and maintains memoranda of agreement (MOAs) with other nations regarding reciprocity of accreditation acceptance. The institute researches, studies, and advises agencies of information technology (IT) vulnerabilities and develops techniques for the cost-effective security and privacy of sensitive Federal systems. NIST guidance aides in improving information systems security by raising awareness of IT risks, vulnerabilities, and protection requirements, and provides measures and metrics based on the guidance provided in a full risk management framework.

Academia, Research Centers, and Think Tanks

- **National Research Council, Transportation Research Board (TRB).** TRB facilitates the sharing of information on transportation practices and policy by researchers and practitioners, providing expert advice on transportation policy and programs, including security and infrastructure protection policy and program development.
- **U.S. Coast Guard Research and Development Center.** The center is the USCG's sole facility for performing research, development, test and evaluation (RDT&E) in support of USCG's missions, including homeland security.
- **National Laboratories and Technology Centers.** DOE's National Infrastructure Simulation and Analysis Center (NISAC), at Los Alamos National Laboratory, provides advanced modeling and simulation capabilities for analyzing critical infrastructures and their interdependencies, vulnerabilities, and complexities.
- **Multidisciplinary Center for Earthquake Engineering Research (MCEER).** MCEER comprises a consortium of researchers and industry partners from numerous disciplines and institutions throughout the United States. MCEER's mission addresses the technical and socio-economic impacts of a variety of hazards, both natural and manmade, on critical infrastructure, facilities, and society.
- **Homeland Security Centers of Excellence (HS-Centers).** Through the HS-Centers program, DHS invests in university-based partnerships to develop centers of multidisciplinary research where important fields of inquiry can be analyzed and best practices developed, debated, and shared. HS-Centers bring together the Nation's best experts and focus its most talented researchers on a variety of threats that include those related to the transportation network.
- **The John A. Volpe National Transportation Systems Center (Volpe Center).** DOT RITA's Volpe Center is an internationally recognized center of transportation and logistics expertise. The Volpe Center assists Federal, State, and local governments, as well as industry and academia in areas including human factors research; system design, implementation, and assessment; global tracking and situational awareness of transportation assets and cargo; and strategic investment. The Volpe Center's Federal staff, supplemented, as needed, by a cadre of support contractors, provide technical expertise conducting assessments of transportation systems, related critical infrastructures, and government facilities—identifying vulnerabilities, risks, and opportunities to improve safety, physical and information systems security, resilience, and operational efficiency—on behalf

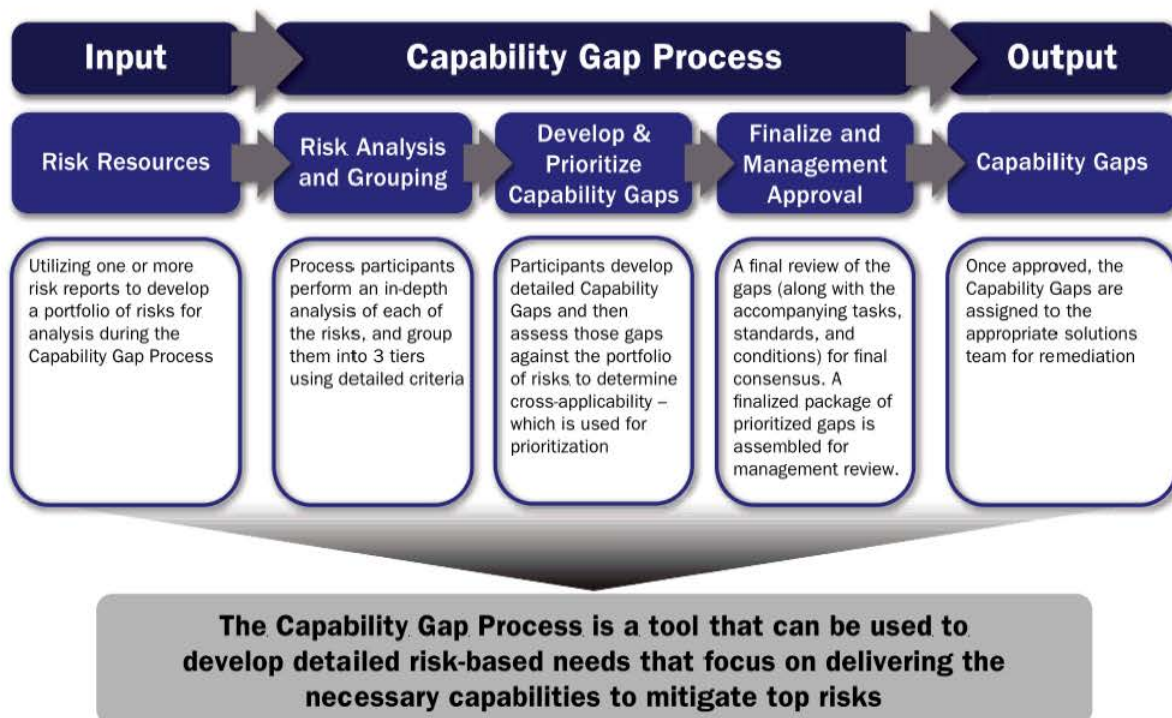
of DOT, DoD, DHS, DOS, and other sector partners. These activities are accomplished through the examination, evaluation, and testing of innovative technologies, policies, procedures, organizational improvements, or a combination of these, and by the design, rapid prototyping, and deployment of integrated solutions, including the development of information management systems which support the assessment of transportation security threats, vulnerabilities, risks, and their associated mitigation strategies.

- **Homeland Security Institute (HSI).** HSI's mission is to assist DHS S&T Directorate and DHS Operating Elements in addressing important homeland security issues, particularly those requiring scientific, technical, and analytical expertise.
- **Turner Fairbank Highway Research Center (TFHRC).** TFHRC is the research arm of FHWA conducting research in all aspects of highways including safety appurtenances, intelligent transportation systems, bridges and other highway structures, pavements, and human factors. Research is conducted in-house through its 22 laboratories and off-center through contract and cooperative research programs. It also collaborates with national and international laboratories in conduct of work. The TFHRC answers to the needs of the States' Departments of Transportation and provides products to develop a safer and more reliable highway transportation system for the general public.

Appendix 5: The Capability Gap Process

The Capability Gap Process is a methodology used to support development of risk-based needs and decisionmaking within an organization. Using information from various sources such as risk, vulnerability, and intelligence reports, the process focuses on assessing current abilities to mitigate top risks, and identify specific gaps within current practices. The identified gaps are then prioritized using specific criteria, and routed to the appropriate resources for solution development. This process ensures that the solutions and actions taken for risk reduction are derived from credible risk sources.

Figure A5-1: Capability Gaps Process



Process Inputs

To develop risk-based needs, the Capability Gap Process uses information from multiple risk and vulnerability reports. Multiple resources are used in order to provide different perspectives while minimizing the possibility of analytical error in any single source. Once the top risks are selected for evaluation, they are presented to participants in a format further described below.

Collaborative and Credible Participants—The Capability Gap Workshops provide an environment where participation and collaboration is necessary. Each agency identifies participants in this process by selecting knowledgeable personnel who represent a broad set of stakeholders and can provide the necessary subject matter expertise. Participants are responsible for developing, evaluating, and prioritizing capability gaps and validating capability gap packages for leadership review. A possible, illustrative membership structure is depicted below:

Table A5-1: Capability Workgroup Participants

Capability Workgroup Participants	
Resources	Expected Participants
FSD	4
OSO Innovation Resource	1
OST Resource	1
Office of Intelligence Resource	1
Planning and Programs Resource	1
Office of Operational Improvement	1

Since the Capability Gap Process is collaborative and involves qualitative analysis, differing opinions and disagreements are expected. Therefore, an organized dispute process is used to make most efficient use of time allotted to each session. A facilitator is responsible for declaring if consensus is reached during a dispute, or if the issue is to be set aside for further analysis. If further analysis is needed, the vote outcomes and minority opinions are noted and summarized at the end of each session.

Capability Gap Process

The Capability Gap Process employs three sessions to discuss and evaluate risks, develop a comprehensive and prioritized list of capability gaps, and create a finalized package for management review and assignment. As a result, the workshops yield a final set of risk-based capability gaps and initial requirements for solution development.

Session I: Risk Analysis and Grouping

Part 1: Introduction to Risks—The first part of Session I serves as an information session to developing an understanding among workgroup participants of the overall Capability Gap Process and the initial evaluation set of risks that will be used in the process. The evaluation set of risks are described as stemming from various risk sources and assessments. Since the risks being presented to the Capability Gap Workshop participants have been designated as High through various reports, there is a need to tier these risks using more detailed, qualitative criteria, which will be later used for capability gap prioritization.

Part 2: Risk Grouping—During the second part the participants analyze the current risk portfolio and perform a risk grouping exercise. Each risk is mapped to a nodal diagram depicting the path of attack that an adversary would likely follow for execution. The attack path may also highlight other information such as current countermeasures and previously identified capability gaps (where a solution may already be under development). This information provides participants greater information to use while creating capability gaps.

After reviewing each nodal diagram and risk description, the risk grouping method occurs using the following set of detailed, qualitative criteria:

Criteria	Description	Rating System
Magnitude of Consequence	Refers to a particular risk/threat scenario's perceived consequence (loss of life, social, and economic impacts) if an attack is carried out successfully.	Tier 1 Tier 2 Tier 3
Adversary Resource Requirements	Refers to the complexity of effort required by the attacker to exploit a specific risk.	Simple Moderate Complex
Professional Judgment	Refers to the personal judgment of workshop participants who have expertise in the field. Participants are asked: "Does this risk keep you awake at night based on operational experience and analysis?"	Grave Concerned Low Concern
<p>* The grouping of risks using the criteria above is not to serve as a method for additional prioritization, as all risks being considered are typically "High" from their respective sources. Instead, the criteria for grouping are only used for the prioritization of Capability Gaps.</p> <p>** The rating systems for each criterion are listed in order from highest to lowest (top-down). For Adversary Resource Requirements, Simple indicates that the resources are easy to obtain to execute a given risk.</p>		

The combination of criteria assessments will provide the final grouping of the evaluated risks, which supports the process for gap prioritization.

Part 3: Introduction to Capability Gaps—The final part of Session I focuses on providing workshop participants with the proper tools for creating high-quality descriptions of capability gaps. This includes providing definitions around key terminology, the relationships between capability gaps and risks, and detailed examples showing how to write a satisfactory capability gap. The TSA Capability Gap Form will be provided for participants to use as a template in writing a new capability gap. This form provides areas to describe the gap and identify the desired outcome, end users, and appropriate risk coverage. It also elicits various tasks, standards, and conditions that must be accomplished in order to address the gap. These tasks, standards, and conditions become the requirements used in solution development. An example of the Capability Gap Form is depicted below:

Figure A5-2: Capability Gap Form

TSA CAPABILITY GAP FORM

Capability Gap Title	
Identification Number	
Description of Capability Gap Please explain the existing gap in current capabilities. This can include: <ul style="list-style-type: none"> ➤ Type of threat(s) needed to be addressed ➤ Aviation sector (e.g. Air Cargo, Passenger Screening...) ➤ Gaps in existing capabilities ➤ Location(s) where gap exists 	
Desired Outcome Please provide the desired outcome for addressing this capability gap. This may include: <ul style="list-style-type: none"> ➤ Desired performance levels ➤ Possible location(s) of capability ➤ Integration/interaction with other existing capabilities 	
Risk Coverage Indicate the risk(s) that this capability gap will address.	
End User Identification	
Tasks What tasks must be completed to perform/utilize this capability?	
Conditions Please indicate the conditions in which this must perform.	
Standards What are the minimum performance standards?	
Other Please provide any additional information that may be useful for the development of this capability.	

In addition, workgroup participants are divided into sub-groups to practice writing a satisfactory capability gap. Each participant is then assigned one or more risks and to individually draft a capability gap(s) to address those risks prior to Session II.

Session II: Develop and Prioritize Capability Gaps

Parts 1-3: *Capability Gap Workshop*—The entirety of Session II reviews and assesses each capability gap as written by a workgroup participant. All participants present their drafted capability gaps to the group to facilitate feedback and discussion. Individuals then reassess their capability gaps and refine drafts to include precise language and appropriate specificity.

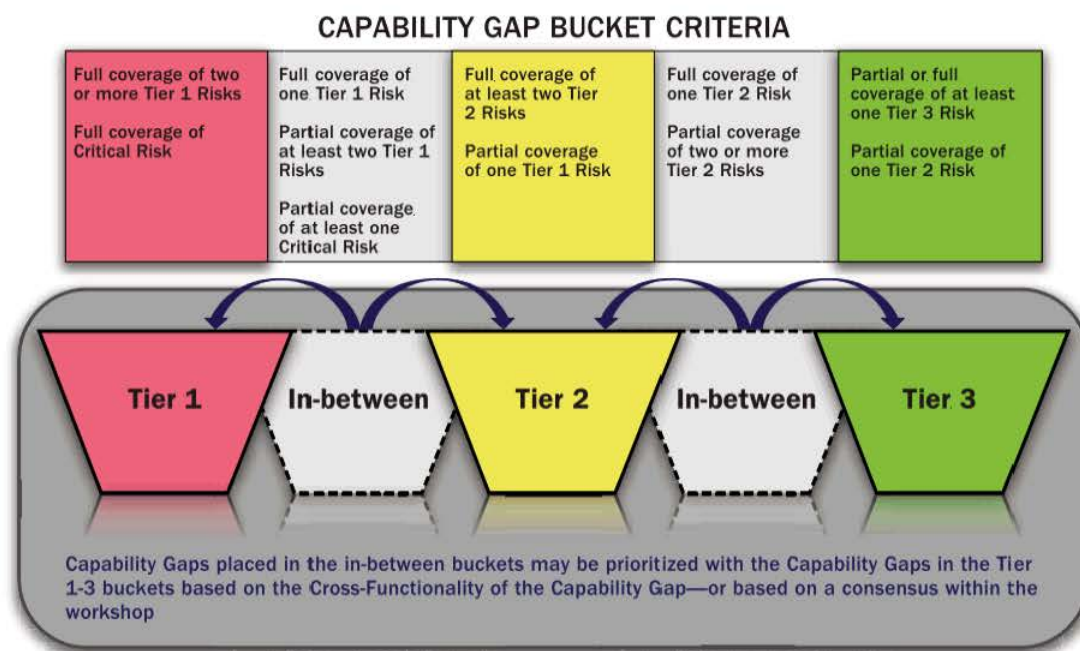
Once the gaps are revised, they are assessed across the previously identified risk groups. The prioritization process is based on criteria that take into account both the grouping of the risks they address as well as the number of risks they cover. Thus, higher importance is placed on capability gaps that cover a large number of Tier I risks. The prioritization matrix allows participants to visually identify the appropriate capability gap-to-risk relationships. These relationships are shown below:

Table A5-2: Capability Gaps to Risk Relationships

Coverage Level	Description
No Coverage	The scope of the capability gap does not address the risk. <i>Example: A capability gap that addresses the inability to detect one type of weapon at a checkpoint will not encompass the risk of a different type of weapon being carried onto a plane.</i>
Partial Coverage	The scope of the capability gap partially addresses the risk. (Closing this gap could result in an estimated 1-10% reduction in risk.) <i>Example: A capability gap that addresses the inability to scan a specific item at a checkpoint might moderately address the risk of a specific type of weapon being carried onto a plane.</i>
Full Coverage	The scope of the capability gap completely addresses the risk. (Closing this gap could result in an estimated 10% or more reduction in risk.) <i>Example: A capability gap that addresses the lack of full-body scanning at the checkpoint will fully encompass the risk of a specific type of weapon being carried onto a plane.</i>

Ultimately, the capability gap to risk relationship determines a capability gap's cross-applicability and places it into a High, High-Medium, Medium, Medium-Low, or Low prioritization bucket. An illustrative view of the capability gap prioritization bucket is depicted below:

Figure A5-3: Capability Gap Bucket Criteria



After the final prioritization, workshop participants perform a final qualitative review to ensure the results are aligned with original intent.

Session III: Finalize Capability Gaps and Prepare for Management Approval

Part 1: Validate and Finalize—The final session reviews the top priority capability gaps that will continue in the solution development process. Each capability gap is validated for accuracy and completeness. The recommended solution ownership groups that are presented for each capability gap are also reviewed and verified by workgroup participants and management.

Output

Following Session III, the top priority capability gaps are finalized and approved by management. The tasks, standards, and conditions of each capability gap ultimately become the initial capability gap requirements for a particular solution. After the capability gaps are finalized and approved by management, they are distributed to the appropriate resource(s) (such as the R&DWG) for solution development and deployment.

Appendix 6: Taxonomy

Reference Number	NAICS CODE	DESCRIPTION
11	TRANSPORTATION	
	<p>The Transportation Systems Sector is comprised of a multitude of network of transportation systems. Systems vary in size and complexity, but all modes of transportation have one element in common; they have defined origin and destination points, and the assets that comprise the systems of interest exist for the sole purpose of facilitating the flow of either people or products. For the purposes of this taxonomy, assets are comprised of nodes and linkages. One example of a node is a rail yard; one example of a link is the stretch of rail track that joins two rail yards. Hence, users of the transportation portion of this taxonomy must first think in terms of specifically defined systems and the flow of either people or products through the defined systems. The individual assets provided in this taxonomy, then, are the physical elements that comprise the systems of interest.</p>	
11.1	AVIATION	
	Assets involved in the aviation industry	
11.1.1	481	Aviation Conveyances
		Includes all types of aircraft.
11.1.2	488119	Airports
		Fields for handling aircraft landings and takeoffs.

Reference Number	NAICS CODE	DESCRIPTION
11.1.2.1		Certificated Airports
		Airports that hold certificates under Federal regulations (14 CFR Part 139). Includes runways, taxiways, apron areas, passenger terminals, baggage handling areas, cargo terminals, maintenance facilities, parking lots and garages, customs and immigration facilities (if handling international flights), and other ancillary service facilities. Using the applicability paragraph of Part 139, a certificated airport (11.1.2.1) is defined as "Any airport in any State of the United States, the District of Columbia, or any territory or possession of the United States serving any (1) Scheduled passenger-carrying operations of an air carrier operating aircraft designed for more than 9 passenger seats, as determined by the aircraft type certificate issued by a competent civil aviation authority and (2) Unscheduled passenger-carrying operations of an air carrier operating aircraft designed for at least 31 passenger seats, as determined by the aircraft type certificate issued by a competent civil aviation authority. Included are those portions of a joint-use or shared-use airport that are within the authority of a person serving passenger-carrying operations. This does not include (1) Airports serving scheduled air carrier operations only by reason of being designated as an alternate airport (2) Airports operated by the United States (3) Airports located in the State of Alaska that only serve scheduled operations of small air carrier aircraft and do not serve scheduled or unscheduled operations of large air carrier aircraft (4) Airports located in the State of Alaska during periods of time when not serving operations of large air carrier aircraft or (5) Heliports.
11.1.2.2	488119	Non-Certificated Airports
		Airports that do not hold certificates under Federal regulations (14 CFR Part 139). Includes runways, taxiways, apron areas, and other facilities. Using the applicability paragraph of Part 139, a non-certificated airport (11.1.2.2) is defined as "Any airport with scheduled passenger-carrying operations of an air carrier operating aircraft designed for 9 or less passenger seats or unscheduled passenger-carrying operations of an air carrier operating aircraft designed for 30 or less passenger seats and includes (1) Airports serving scheduled air carrier operations only by reason of being designated as an alternate airport (2) Airports operated by the United States (3) Airports located in the State of Alaska that only serve scheduled operations of small air carrier aircraft and do not serve scheduled or unscheduled operations of large air carrier aircraft (4) Airports located in the State of Alaska during periods of time when not serving operations of large air carrier aircraft or (5) Heliports."
11.1.2.3	928110	Military Airfields
		Airfields owned and operated by the military. Includes runways, taxiways, apron areas, maintenance and other facilities.
11.1.2.4	(488119)	Foreign Airports
		Airports outside the U.S.
11.1.3	488111	Air Traffic Control and Navigation Facilities
		Includes control centers, radar installations, and communication facilities. Facilities that provide information (e.g., weather, route, terrain, flight plans) for private pilots flying into and out of small airports and rural areas. Also assists pilots in emergencies and coordinates search-and-rescue operations for missing or overdue aircraft.

Reference Number	NAICS CODE	DESCRIPTION
11.1.3.4	488111	Other Air Traffic Control Facilities
		Facilities not elsewhere classified or future facilities.
11.1.4		Space Transportation Facilities
11.1.4.1		Military Facilities
11.1.4.2		Commercial Facilities
		Spaceports and facilities for the processing, integration, and assembly of civilian and commercial orbital and suborbital launch vehicles and payloads, launch and recovery operations, and range support for civilian and commercial space activities.
11.1.4.3	927110	NASA Facilities
		Spaceports and facilities for the processing, integration, and assembly of NASA orbital and suborbital launch vehicles and payloads, launch and recovery operations, and range support for NASA space activities.
11.1.5		Aviation Sector Command Control Communication Coordination Facilities
		Facilities involved in providing, maintaining, or restoring a safe and secure aviation system. Includes facilities such as FAA Air Traffic Control System Command Center, National Capitol Region Command Center, Transportation Security Operations Center, and NORAD Cheyenne Mountain Operations Center.
11.1.6		Other Aviation Facilities
		Aviation facilities not elsewhere classified.
11.2	RAILROAD	
		Assets involved in rail transportation.
11.2.1	48211	Railroad Conveyance
		Includes all types of trains.
11.2.1.1	48211	Freight Conveyance
		Trains that handle the movement of goods from producer to consumer.
11.2.1.2	48211	Passenger Conveyance
		Trains that handle the movement of people by rail.

Reference Number	NAICS CODE	DESCRIPTION
11.2.2	48211	Railroad Rights-of-Way
		Routes along which trains operate.
11.2.2.1	48211	Railroad Track
		Includes main line tracks, sidings, switches, crossovers.
11.2.2.2	48211	Railroad Bridges
		Bridges carrying rail traffic. May also carry commuter rail traffic and/or road traffic.
11.2.2.3	48211	Railroad Tunnels
		Tunnels carrying rail traffic. May also carry commuter rail traffic and/or road traffic.
11.2.3	48211	Railroad Yards
		Areas having a network of tracks and sidings for handling cars.
11.2.3.2	48211	Rail Yard - Classification
		A railroad yard with special facilities to efficiently group rail cars according to destination to facilitate the makeup and breakdown of trains. May have areas adjacent for the loading/unloading of cars.
11.2.3.3	48211	Rail Yard - Intermodal
		A railroad yard that is used specifically for handling the transfer of containers and/or trailers between trains and other modes of transport (e.g., truck, ship). Note Included in this category are facilities that have the label "Inland Port." These facilities, in spite of the label, handle rail-to-road transfers. They are labeled Inland Ports since all traffic moves to and from the facility by rail to the marine docks.
11.2.3.4	48211	Rail Yard - HAZMAT
		A railroad yard that has special facilities for handling hazardous materials.
11.2.4	48211	Railroad Stations
		Sites along and at the end of rail lines to which service is provided.
11.2.4.1	48211	Railroad Passenger Stations
		Sites along or at the end of rail lines for the boarding of Passengers on trains for either Long Distance/Intercity trains or Commuter trains. May include connections to heavy rail, light rail, mass transit, urban rapid transit, buses, or other modes of transport.

Reference Number	NAICS CODE	DESCRIPTION
11.2.5	48211	Railroad Operations Centers
		Facilities to provide operational control of railroads.
11.2.5.1	48211	Railroad Dispatch and Operations Control Centers
		Facilities where railroad personnel monitor and control the movement of trains.
11.2.5.2	48211	Railroad Communications Centers
		Facilities and equipment where railroad communications are handled.
11.2.5.3	48211	Railroad Signaling Facilities and Equipment
		Facilities and equipment used to control signals used to direct train traffic.
11.2.6		Other Railroad Facilities
		Railroad facilities not elsewhere classified.
11.3	ROAD	
		Assets involved in road transportation.
11.3.1		Roadways and Supporting Facilities
		Facilities supporting road transport.
11.3.1.1	(2373)	Roadways
		Highways and roads for motor vehicles. Note: Some roads are designated as part of the Strategic Highway Network (STRAHNET).
11.3.1.2	(488490)	Road Bridges
		Bridges carrying road traffic. May also carry rail and/or pedestrian traffic.
11.3.1.3	(488490)	Road Tunnels
		Tunnels carrying road traffic. May also carry rail and/or pedestrian traffic.
11.3.1.4	(2373)	Highway Rest and Service Areas
		Service facilities attached to highways.
11.3.1.5		Road Transportation Support Facilities
		Facilities providing supporting services to road transportation.

Reference Number	NAICS CODE	DESCRIPTION
11.3.2		Trucking
		Vehicles and facilities related to freight movement by truck.
11.3.2.1	484	Truck Conveyance
		Includes all types of trucks.
11.3.2.2		Truck Terminals
		Facilities operated by a trucking company handle a large number of truck arrivals and departures. Used for handling and temporary storage of freight pending transfer to other locations. In general, freight is stored at a terminal for relatively short periods (e.g., hours, days). Less-than-truckload (LTL) terminals have buildings where smaller quantities of freight are broken apart and reassembled based on destination. Truckload (TL) facilities handle only full truckloads and typically have large open spaces for truck parking and possibly small or no buildings. Both LTL and TL terminals generally have truck maintenance facilities.
11.3.2.3	532120	Truck Rental Facilities
		Establishments primarily engaged in renting or leasing, without drivers, trucks, truck tractors, or semitrailers.
11.3.2.4	484	Truck Dispatch Centers
		Facilities where communication equipment is located, trucks are dispatched, and fleet operations are coordinated.
11.3.2.5	484	Truck Operations Centers
		Facilities where communication equipment is located, trucks are dispatched, and fleet operations are coordinated.
11.3.3	485210	Over-the-Road Motorcoach System
		Bus system providing service principally outside a single metropolitan area and its adjacent nonurban areas. Includes both regularly scheduled and charter bus service. Does not include urban mass transit bus systems or school bus services, which are classified under mass transit.
11.3.3.1	485210	Motorcoach Conveyance
		Includes all types of buses.
11.3.3.2	485210	Over-the-Road Motorcoach Passenger Terminals
		Terminals designed to board and unload passengers and luggage. May be a dedicated facility (e.g., in an urban area) or may be a drop-off point (e.g., in a rural area). May have multi-modal facilities (e.g., rail, mass transit).

Reference Number	NAICS CODE	DESCRIPTION
11.3.3.3	485210	Over-the-Road Motorcoach Facilities
		Parking and maintenance facilities for buses. Facilities where routine and specific maintenance is performed on Over-the-Road Motorcoaches.
11.3.3.4	485210	Over-the-Road Motorcoach Operations Centers
		Facilities where communication equipment is located, buses are dispatched, and fleet operations are coordinated.
11.3.3.5	485210	Over-the-Road Motorcoach Dispatch Centers
		Facilities where communication equipment is located, buses are dispatched, and fleet operations are coordinated.
11.3.4	485113	School Bus Systems
		Bus transportation systems for transport of children to and from school and school-related events.
11.3.4.1	485113	School Bus Conveyance
		Includes all types of school buses.
11.3.4.2	485113	School Bus Routes
		Routes followed by school buses. Usually streets shared with other vehicles and pedestrians.
11.3.4.3	485113	School Bus Stops
		Stops for loading and unloading children. May be in a terminal with connections to other transport modes.
11.3.4.4	485113	School Bus Maintenance Facilities
		Storage and maintenance facilities for school buses.
11.3.4.5	485113	School Bus Dispatch Centers
		Facilities where school bus personnel monitor and control the movement of buses.
11.3.4.6	485113	School Bus Communication Centers
		Facilities where communication equipment is located and school bus fleet operations are coordinated.

Reference Number	NAICS CODE	DESCRIPTION
11.3.5		Other Road Facilities
		Road transportation facilities not elsewhere classified.
11.4	MARITIME	
		Assets involved in the movement of passengers and freight by water.
11.4.1		Vessels
		Includes marine vessels.
11.4.1.1	(483)	Shallow Draft Vessels
		Vessels with less than 15 ft draft. <i>Barges designed to carry gaseous materials.</i>
11.4.1.2	(483)	Deep Draft Vessels
		Vessels with draft equal to or more than 15 feet.
11.4.2	488310	Ports
		Facilities designed to dock, load, and unload marine vessels.
11.4.2.1	488310	Shallow Draft Ports
		Ports capable of handling vessels with drafts less than 15 feet.
11.4.2.2	488310	Deep Draft Ports
		Ports capable of handling vessels with drafts of 15 feet or more.
11.4.2.3	488310	Port Public Access Areas
		Public gathering places in a port, such as parks, fishing piers, dining/shopping sites, etc. May have large numbers of people gathered for events.
11.4.2.4	488310	Public Access Areas
11.4.3		Military and Strategic Seaports
11.4.3.1		Military and Strategic Deep Draft Ports
11.4.4		Waterways
		Navigable waterways capable of carrying marine traffic.

Reference Number	NAICS CODE	DESCRIPTION
11.4.4.1	(4832)	Inland Waterways
		Natural waterways (e.g., rivers, lakes, bayous, estuaries) capable of carrying marine traffic.
11.4.4.2	(4832)	Intracoastal Waterways
		Partly natural, partly manmade waterways providing sheltered passage for commercial and leisure boats along the U.S. Atlantic coast and along the Gulf of Mexico coast.
11.4.4.3	(4832)	Navigation Locks
		Walled section of a river or canal, closed by water gates at both ends, in which the water level can be raised or lowered by means of valves or sluiceways to match the level in the upper or lower reach, as desired. When the levels are the same, the water gate is opened to permit a vessel to enter or leave the lock.
11.4.4.4	(4832)	Canals
		A constructed channel, usually open, that conveys water by gravity to farms, municipalities, etc. Artificial watercourse of perceptible extent, with a definite bed and banks to confine and conduct continuously or periodically flowing water.
11.4.4.5	(4832)	Dams
		Water retention structures used for irrigation, electricity generation, water supply storage, flood control, navigation, fisheries, recreation, sediment and hazardous materials control, or mine tailings impoundments. Many dams have multiple uses.
11.4.5	488330	Maritime Supporting Facilities
		Facilities supporting the operation of marine vessels.
11.4.5.1	488330	Navigation Facilities
		Facilities providing marine navigation support.
11.4.5.2		Emergency Search and Rescue Facilities
		Facilities equipped to respond to maritime emergencies.
11.4.6		Other Maritime Facilities
		Maritime transportation facilities not elsewhere classified.
11.5	MASS TRANSIT	
	Mass transportation (mass transit) means transportation by a conveyance that provides regular and continuing general or special transportation to the public, but does not include school bus, charter, or sightseeing transportation.	

Reference Number	NAICS CODE	DESCRIPTION
11.5.1	485119	Rail Mass Transit
		Rail mass transit is the system for carrying transit passengers described by specific right-of-way, technology, and operational features.
11.5.1.1	485119	Rail Transit Cars
11.5.1.2	485119	Rail Transit Passenger Stations
		A station on a rail transit line that provides passenger loading and unloading. May be above or below ground. May connect with other modes of transport.
11.5.1.3		Rail Transit Rights-of-Way
		Includes rail transit track, bridges, and tunnels.
11.5.1.4		Rail Transit Yards
		Areas having a network of tracks and sidings used primarily for makeup, breakdown, storage, and maintenance of trains.
11.5.1.5		Rail Transit Dispatch and Operations Control Centers
		Facilities where rail transit personnel monitor and control the movement of trains.
11.5.1.6		Rail Transit Communications Centers
		Facilities and equipment where rail transit communications are handled.
11.5.1.7	485119	Rail Transit Signaling Facilities and Equipment
		Facilities and equipment to signal trains and direct traffic of trains in transit.
11.5.2	485113	Bus Mass Transit
		Mass transit operating fixed routes and schedules on streets shared with other vehicles and pedestrians.
11.5.2.1	485113	Transit Bus Vehicles
		Includes bus-vehicles powered by diesel, gasoline, battery or alternative fuel engines contained within the vehicle. Can be single unit or articulated. Trolleybus-vehicles propelled by a motor drawing current from overhead wires via a connecting pole called a trolley from a central power source not on board the vehicle.
11.5.2.2	485113	Transit Bus Routes
		Routes followed by transit buses. Usually streets shared with other vehicles and pedestrians.

Reference Number	NAICS CODE	DESCRIPTION
11.5.2.3	485113	Transit Bus Terminals
		(Also called bus stations or bus depots.) Central facilities or hubs for buses to load and unload passengers. May have connections to other transport modes.
11.5.2.4	485113	Transit Bus Stops
		Stops for loading and unloading passengers. May have a shelter.
11.5.2.5	485113	Transit Bus Garages
		Storage and maintenance facilities for transit buses.
11.5.2.6	485113	Transit Bus Dispatch and Operations Control Centers
		Facilities where transit bus personnel monitor and control the movement of buses.
11.5.2.7	485113	Transit Bus Communication Centers
		Facilities and equipment where bus communications are handled.
11.5.3		Other Mass Transit Systems
		Mass transit facilities not elsewhere classified.
11.6	PIPELINES	
		Pipelines for transporting liquids and gases. Includes petroleum and natural gas pipelines (both of which are also itemized in the Energy Sector), hazardous chemicals (also itemized in the Chemical and Hazardous Materials Sector), and other liquids and gases.
11.6.1	486110	Crude Oil Pipelines
		Pipeline facilities for the transport of crude oil.
11.6.1.1	486110	Crude Oil Pipeline Components
		Lengths of pipeline, interconnections, valves. Includes above ground, underground, river crossings, and other segments.
11.6.1.2	486110	Crude Oil Pipeline Pumping Stations
		Stations along the length of a pipeline. Includes pumps, valves, control machinery, breakout storage.
11.6.1.3	486110	Crude Oil Pipeline Control Centers
		Central control facilities that monitor and operate a pipeline(s). Includes SCADA system control centers.

Reference Number	NAICS CODE	DESCRIPTION
11.6.1.4	424710	Crude Oil Storage
		(Also referred to as tank farms.) Facilities used for the storage and/or marketing of crude oil. Includes storage tanks, pipes and pumps, control machinery, and other equipment. Does not include storage at refineries.
11.6.1.5		Crude Oil Pipeline Hub
		(Also known as a Market Center.) A market or supply area for pooling and delivery of Crude Oil where transactions occur to facilitate the movement of crude oil between and among inter-state pipelines. Transactions can include a change in title of crude ownership, a change in crude transporter, or other similar items.
11.6.2	486910	Petroleum Product Pipelines
		Pipeline facilities for the transport of petroleum products.
11.6.2.1	486910	Petroleum Product Pipeline Components and Interconnects
		Lengths of pipeline, interconnections, valves. Includes above ground, underground, river crossings, and other segments. Facilities that link one company to another company to transfer products custody or provide emergency transportation service between companies. This includes facilities such as pipeline segments, valves, or pressure reduction stations.
11.6.2.2	486910	Petroleum Product Pipeline Pumping Stations
		Stations along the length of a pipeline. Includes pumps, valves, control machinery, breakout storage.
11.6.2.3	486910	Petroleum Product Pipeline Control Centers
		Central control facilities that monitor and operate a pipeline(s). Includes SCADA system control centers.
11.6.2.4	486910	Petroleum Product Storage
		(Also referred to as tank farms.) Facilities used for the storage and/or marketing of petroleum products. Includes storage tanks, pipes and pumps, control machinery, and other equipment. Does not include storage at refineries.
11.6.3	48621	Natural Gas Transmission Pipelines
		Large, high-volume pipelines.

Reference Number	NAICS CODE	DESCRIPTION
11.6.3.1	486210	Natural Gas Transmission Pipeline Components and Interconnects
		Lengths of pipeline, interconnections, valves. Includes above ground, underground, river crossings, and other segments. Facilities that link one company to another company to transfer gas custody or provide emergency transportation service between companies. This includes facilities such as pipeline segments, valves, or metering and/or pressure reduction stations.
11.6.3.2	486210	Natural Gas Transmission Pipeline Compressor Stations
		Stations along the length of a transmission pipeline. Includes gas-powered or electric compressors, valves, control systems, and associated equipment.
11.6.3.3	486210	Natural Gas Transmission Pipeline Control Centers
		Central control facilities that monitor and operate a transmission pipeline(s). Generally includes SCADA system control equipment.
11.6.3.4	211112	Natural Gas Transmission Storage
		Facilities for storing natural gas.
11.6.3.5	486210	Natural Gas Pipeline Hub
		(Also known as a Market Center.) A market or supply area for pooling and delivery of gas where transactions occur to facilitate the movement of gas between and among interstate pipelines. Transactions can include a change in title of gas ownership, a change in gas transporter, aggregation of gas supply, or other similar items.
11.6.3.6	486210	Natural Gas Receipt/Delivery Metering Stations
		Gas custody transfer metering stations along transmission pipelines. Used to monitor the amount of gas that is transported and to provide quantity measurements for billing purposes.
11.6.3.7	211112	Liquefied Natural Gas Storage (Terminal)
		Facilities that store LNG and regasify it for injection into pipelines. Includes specially designed tanks to store the LNG.
11.6.4		Natural Gas Distribution
		Facilities, generally owned by local distribution companies (LDCs), to distribute natural gas to final consumers.
11.6.4.1	486210	City Gate Stations
		Measuring, custody transfer, and pressure regulating stations where a natural gas distribution company receives gas from a transmission company and where pressure is reduced and odorant is added to meet distribution network requirements.

Reference Number	NAICS CODE	DESCRIPTION
11.6.4.2	221210	Natural Gas Distribution Pipeline Networks
		The network of lower pressure pipelines that provide natural gas to consumers.
11.6.4.3	221210	Natural Gas Distribution Control and Dispatch Centers
		These centers control the lower pressure gas distribution system. Includes distribution SCADA systems.
11.6.4.4	211112	Natural Gas Distribution Storage
		Facilities for storing natural gas for peak shaving and distribution.
11.6.5	(483)	LNG Transport
		Facilities to move liquefied natural gas.
11.6.5.1	483	LNG Tankers
		Specially-designed ships for carrying LNG and maintaining very low temperatures. Generally used for imported LNG.
11.6.5.2	488310	LNG Ports
		Port facilities designed to handle LNG tankers. Includes mooring facilities, loading and unloading facilities. Includes specially designed storage tanks. Includes regasification equipment to regasify LNG for injection into pipelines.
11.6.6	48699	Other Pipelines
		Pipelines carrying other liquids or gases.
11.6.6.1	48699	Other Pipeline Components
		Lengths of pipeline, interconnections, valves. Includes above ground, underground, river crossings, and other segments.
11.6.6.2	48699	Other Pipeline Pumping Stations
		Stations along the length of a pipeline. Includes pumps, valves, control machinery, breakout storage.
11.6.6.3	48699	Other Pipeline Control Centers
		Central control facilities that monitor and operate a pipeline(s). Includes SCADA system control centers.

Reference Number	NAICS CODE	DESCRIPTION
11.6.6.4	48699	Other Pipeline Terminals
		Facilities where multiple pipelines interconnect. May include storage facilities where material being transported is stored temporarily.
11.6.7		Other Pipeline Facilities
		Not elsewhere classified.
11.7		REGULATORY, OVERSIGHT, AND INDUSTRY ORGANIZATIONS
		Organizations that provide technical, operation, pricing, and business oversight and support to the various components of the transportation system.
11.7.1		Federal Transportation Agencies
		Federal agencies dealing with transportation including Department of Transportation, Federal Aviation Administration; Department of Homeland Security, U.S. Coast Guard, Transportation Security Administration, U.S. Army Corps of Engineers, etc.
11.7.2		State, Local, Regional Transportation Agencies
		State, local, and regional agencies that deal with transportation in their jurisdictions.
11.7.3		Transportation Industry Organizations
		Industry organizations that provide industry-wide support.
11.7.4		International Transportation Organizations
		International organizations dealing with transportation issues.



Modal Annexes



Annex A: Aviation



Contents

1. Executive Summary	127
2. Overview of Mode	129
2.1. Vision of Mode	129
2.2. Description of Mode	129
2.3. Aviation Modal Partnerships	131
2.3.1. Federal Aviation Partners	131
2.3.2. Aviation Modal Partnership Framework	133
2.4. Risk Management	133
2.4.1. Risk Profile	133
2.4.2. Aviation Threat Categories	134
2.4.3. Aviation Modal Risk Assessment Process	135
2.4.4. Risk Management Analysis Process	136
2.4.5. Risk Mitigation Strategy	136
3. Implementation Plan	139
3.1. Goals, Objectives, and Programs/Processes	139
3.1.1. Goal 1: Prevent and Deter Acts of Terrorism Using or Against the Transportation System	139
3.1.2. Goal 2: Enhance the All-Hazard Preparedness and Resilience of the Aviation Transportation System to Safeguard U.S. National Interests	141
3.1.3. Goal 3: Improve the Effective Use of Resources for Transportation Security	144
3.1.4. Goal 4: Improve Situational Awareness, Understanding, and Collaboration Across the Aviation Transportation System	147
3.2. Security Guidelines, Requirements, and Compliance and Assessment Processes	149
3.2.1. Security Guidelines	149
3.2.2. Security Requirements	149
3.2.3. Compliance and Assessment Processes	151
3.3. Decisionmaking Factors	152
3.3.1. Program Implementation	152
3.3.2. Grant Programs	153
3.3.3. Aviation Modal Plan Review Process	153
3.4. Performance Measurement	154
3.4.1. Risk Mitigation Activities	154
3.4.2. Metrics	155

4. Way Forward	157
4.1 Long-Term Aviation Objectives	157
4.2 Near-Term Aviation Objectives	158

Appendix 1: Matrix of Aviation Programs and Activities	161
--	-----

List of Figures

Figure A2-1: Layered Approach to Aviation Security	137
--	-----

List of Tables

Table A2-1: Regulated Components of the Aviation Mode	130
Table A3-1: Key Aviation Modal Risk Mitigation Activities	154

1. Executive Summary

The Aviation Transportation System (ATS) is a vital component of the Transportation Systems Sector, integrally contributing to the free flow of people and commerce across the globe. Within the aviation mode, the National Airspace System (NAS), international aviation systems, and aviation conveyances and operations serve the United States and its citizens. The significance of these systems and assets underscores the necessity of flexible, unpredictable, and efficient aviation security and protection programs and processes. Federal, State, local, territorial, and tribal government partners work closely with the private industry to develop and implement an effective and comprehensive approach to addressing risk within the ATS. The Aviation Modal Plan, as an annex to the 2010 Transportation Systems Sector-Specific Plan (SSP), details this approach, outlining the goals and objectives that aviation modal partners have set, as well as the programs and processes implemented to fulfill them.

The vision of the ATS, set forth in the Aviation Modal Plan, is to create a secure, resilient, and efficient network of airlines, other aviation operators, airports, personnel, and infrastructure that ensures the safe and expedient movement of people and cargo while protecting the civil liberties of all individuals. The layered risk management approach implemented by aviation modal partners utilizes the National Infrastructure Protection Plan (NIPP) risk management framework to strategically align resources to programs and initiatives with the highest contributions to risk reduction and mitigation.

This plan serves as an update to the 2007 SSP Aviation Modal Plan and as a reflection of the aviation mode's implementation strategy for the security framework outlined in the 2010 SSP Base Plan. The Aviation Modal Plan was drafted and reviewed by representatives from the Aviation Sector Coordinating Council (ASCC), Aviation Government Coordinating Council (AGCC), relevant government agencies, and other private sector entities. The aviation modal goals and processes outlined in the plan represent the collective ambitions and strategy of the aviation modal partners in addressing the unique and complex risk profile of the ATS. Ultimately, government and private sector aviation modal partners strive to create a system that internalizes a strong security and protection culture, embedding best practices and government requirements into day-to-day operations without significantly impeding private industry and the traveling public.

The security and economic prosperity of the United States depend significantly upon the secure operation of its ATS and safe use of the world's airspace. The vast, open, and interconnected nature of the Transportation Systems Sector and the ATS creates a unique security challenge. Protecting and securing U.S. aviation infrastructure and assets remains a preeminent priority among Federal aviation modal partners, who continue to evaluate and update modal risk management approaches. Given the ever-changing threat environment, Federal aviation modal partners must continually reexamine the programs and policies in place to maximize relevancy and effectiveness. With this in mind, a risk-based approach must be flexible and incorporate all relevant entities, resources, and partners.



2. Overview of Mode

The ATS is comprised of a broad spectrum of infrastructure owned, operated, or regulated by public and private sector entities both within and outside the United States. The core aviation components are the NAS, international aviation systems, and aviation conveyances and operations that serve the United States and its citizens. The mode's main function is to move passengers and cargo (including mail and consumer packages) safely and efficiently within and beyond U.S. borders.

The safety and security of aviation infrastructure are high priorities for the ATS. Guidelines and requirements are developed by international, Federal, State, and local authorities for specific aspects of aviation, passenger, baggage, and cargo operations. This section describes the community of organizations and agencies that share the responsibilities for protecting critical aviation infrastructure and providing for the survivability of the ATS.

2.1 Vision of Mode

The aviation modal vision is a secure, resilient, and efficient network of airlines, other aviation operators, airports, personnel, and infrastructure that ensures the safe and expedient movement of people and cargo while protecting the civil liberties of all individuals.

2.2 Description of Mode

The ATS is vitally important to U.S. prosperity and freedoms. Each day, commercial aviation moves millions of passengers and their bags through U.S. airports. In 2008, with regard to air cargo, U.S. air carriers flew 37.1 billion revenue-ton miles of air cargo – 13.8 billion domestically and 23.3 billion internationally. Historically, general aviation has accounted for more than 77 percent of all flights in the United States. These various segments of the aviation mode are vital to the economy and to the American way of life.

The NAS is the dynamic network of facilities, systems, services, airspace, and routes that support flights within U.S. airspace, including the international airspace delegated to the United States for air navigation services. The Federal Aviation Administration (FAA) regulates and operates this system. Specifically, the NAS includes more than 690 air traffic control (ATC) facilities with associated systems and equipment to provide radar and communication services; more than 19,800 general aviation and commercial aviation airports capable of accommodating an array of aircraft operations; and volumes of procedural and safety information necessary for users to operate in the system. In addition, the NAS includes over 11,000 air navigation facilities and approximately 13,000 flight procedures.

The NAS is intricately connected globally through U.S. and foreign air carriers flying to and from international and general aviation airports. International aviation partnerships support the safety and security of air travel and commerce. Consequently,

regular consultations between international governmental and private sector partners through formal and informal avenues, including the International Civil Aviation Organization (ICAO), bilateral and multilateral agreements, and Group of Eight (G8) nations, facilitate the effective operation of the NAS and the global aviation network.

The basic components of the ATS regulated for security under Title 49 of the Code of Federal Regulations (CFR) are: aircraft operators, air cargo, foreign air carriers, indirect air carriers, commercial airports, general aviation, and flight schools. These are categorically included in five sub-modal divisions described in table A2-1. Extensive rules and regulations apply to aircraft operations in national airspace and around the globe. U.S. security rules are also extended to those foreign airports and air carriers that fly to the United States.

Table A2-1: Regulated Components of the Aviation Mode

Air Cargo	Air cargo includes property tendered for air transportation accounted for on an air waybill. All accompanied commercial courier consignments, whether or not accounted for on an air waybill, are also classified as cargo. The U.S. air cargo network is made up of over 300 domestic and foreign air carriers, approximately 450 domestic commercial airports, numerous international airports in 98 countries, over 4,000 indirect air carriers (freight forwarders), and over a million world-wide shippers.
Commercial Airlines	Commercial airlines are those that engage in regularly scheduled or public charter operations, including domestic air carriers and foreign air carriers flying within, from, to, or over the United States.
Commercial Airports	Commercial airports are defined as airports with regularly scheduled commercial passenger service or public charter operations. There are approximately 450 airports in the United States that are regulated under 49 CFR Part 1542 and have Airport Security Programs.
General Aviation	The general aviation segment of the mode includes any of approximately 19,000 airports, heliports, and landing strips where general aviation aircraft operate including commercial airports as described above. General aviation aircraft are all aircraft except those engaged in military or regularly scheduled commercial operations. General aviation includes diverse industries and operations, including private-use recreational aircraft, business jets, and emergency medical helicopters. General aviation accounts for approximately 77 percent of all flights in the United States.
Flight Schools	Flight schools include any pilot school, flight training center, air carrier flight training facility, flight instructor, or any other person or entity that provides instruction in the operation of any aircraft or aircraft simulator.

Airports, including terminals and supporting facilities, are focal points for multiple transportation modes. Passengers arrive via a variety of ground and air conveyances, cargo moves via trucks into and out of the airport complex, and tankers and delivery vehicles operate continuously with fuel and other supplies serving the needs of the public and businesses in multiple sectors. Dual-use airports serve both military and civilian functions. Thus, aviation system operations provide a vital artery for the functioning of most sectors and for the mobility essential for a resilient economy. These intermodal and cross-sector interdependencies create a dynamic and unique threat environment that requires effective collaboration among aviation modal partners to meet protection and resiliency goals and objectives. To protect aviation assets, systems, and networks modal partners will continue to support and implement multi-modal security enhancements, such as Visible Intermodal Prevention and Response (VIPR) team deployments across the mass transit system, which will strengthen coordination in national and local surface transportation environments, and also continue to work collaboratively to expand these programs internationally.

2.3 Aviation Modal Partnerships

A considerable portion of the Nation's aviation transportation infrastructure is owned and operated by State, local, and tribal governments. These jurisdictions are well positioned to address specific aviation security needs, and preparedness and response capabilities. The State homeland security agencies work with the Federal Government to identify critical transportation assets, conduct vulnerability assessments, develop security and protection plans, improve situational awareness of the traveling public, and train aviation transportation personnel. They also provide primary response and recovery capabilities to address terrorist attacks and other disruptive incidents.

Substantial segments of the Nation's aviation transportation infrastructure are also owned and operated by private sector entities. As such, an effective aviation resiliency strategy must be supported by a private sector that internalizes a strong security and protection culture, embedding best practices and government requirements into day-to-day operations without significantly impeding private industry and the traveling public. It is the responsibility of private sector owners and operators to conduct and execute business continuity planning, integrate security planning with disaster recovery planning, and actively participate with Federal, State, local, territorial, and tribal governments to improve security throughout the ATS. To the maximum extent feasible and appropriate, Federal departments and agencies also coordinate their activities with other aviation modal partners, as well as law enforcement and emergency response agencies to ensure unity of efforts.

2.3.1 Federal Aviation Partners

As a result of the highly regulated nature of the ATS, Federal aviation modal partners must work closely with government agencies and private sector industries in order to achieve the mode's goals and objectives. Federal responsibilities include, but are not limited to:

- Establishing and enforcing regulations, policies, and procedures;
- Providing criminal law enforcement support;
- Identifying potential terrorist threats and appropriate risk-managed countermeasures;
- Sharing critical information and actionable intelligence across various domains;
- Defining and mitigating risks and vulnerabilities on the ground and in the air;
- Providing overall guidance; and
- Applying and/or overseeing security measures, to include extensive passenger and checked baggage screening operations.

The Federal responsibilities for security and protection functions apply to non-travelers, travelers and their carry-on items, checked baggage, cargo, and aviation industry personnel, including staff, vendors, tenants, and flight crews. They impact the operation of foreign and domestic airlines, airports, and the air cargo supply chain. Given the diversity of the mode and wide range of responsibilities, a number of Federal departments and agencies actively collaborate in securing the ATS. The following departments and agencies, however, represent the majority of oversight throughout the ATS:

- **Department of Homeland Security (DHS)**, in accordance with National Security Presidential Directive 47/Homeland Security Presidential Directive 16 (NSPD-47/HSPD-16), which directed the development of the National Strategy for Aviation Security (NSAS), is responsible for closely coordinating U.S. Government activities encompassing national aviation security programs. This responsibility includes evaluating conflicting procedures, identifying vulnerabilities and consequences, coordinating corresponding interagency solutions, and developing a cross-sector risk management approach.
 - **Transportation Security Administration (TSA)** oversees the security of domestic aircraft operators, foreign air carriers, domestic airports, indirect air carriers, and flight schools; provides and supports enforcement of civil and criminal violations; and cooperates with foreign, State, local, territorial, and tribal governments, airport authorities, and law enforcement

agencies, with a special focus on counterterrorism. Intelligence-driven, risk-based strategic, operational, and tactical planning and implementation activities ensure the security of aviation operations, airports, and facilities. TSA screens passengers and checked baggage; operates the Nation's Transportation Security Operations Center (TSOC); deploys Federal Air Marshals (FAMs); assesses the security of domestic and foreign airports; conducts general aviation stakeholder outreach and liaison activities; performs vulnerability assessments of aviation assets; and provides training, public education, and information sharing to enhance the protection of passengers, cargo, and infrastructure. Additionally, teams of transportation security inspectors, principal security inspectors, and international inspectors inspect or audit air carrier compliance with security programs, standards, and regulations. TSA develops, improves, and promotes transportation security programs, processes, and systems worldwide while ensuring achievement of accepted international standards. TSA also supports international aviation security crisis response, capacity building, and management activities; liaises with the Department of State (DOS), Department of Defense (DoD), Department of Transportation (DOT), the ICAO, and other international groups; and deploys aviation security specialists in response to high-threat situations and global security challenges.

- **Customs and Border Protection (CBP)** conducts 24/7 law enforcement multi-domain awareness operations out of the Air and Marine Operations Center (AMOC) in Riverside, CA. CBP leverages the Air and Marine Operations Surveillance System (AMOSS) and extensive intelligence, detection, monitoring, and coordination capabilities to make threat determinations in the performance of critical counterterrorism and counter-narcotics missions primarily focused on general aviation aircraft. In addition, the AMOC creates a common operating picture that Federal, State, and local stakeholders leverage during emergency response and disaster relief efforts, including mission tasking during the Atlantic Hurricane Season, Continuity of Government efforts, or securing the National Airspace for National Special Security Events.
- **Department of Transportation** is responsible for the continual operation and safety of the ATS.
 - **Federal Aviation Administration (FAA)** is the Nation's civil aviation authority and air navigation services provider. It operates and provides regulatory oversight of the NAS. FAA, in cooperation with DHS and other modal partners, plans and implements diverse air traffic and airspace management-related measures to support aviation safety, national defense, homeland security, law enforcement, and incident response. FAA is also responsible for securing manned and unmanned NAS facilities and systems.
- **Department of Justice (DOJ)** is responsible for the ground-based tactical response to hijacking, air piracy, or other terrorist threats; the investigation, enforcement, and prosecution of criminal law violations within its jurisdiction that occur in the ATS; coordinating the law enforcement community; and intelligence collection, counterintelligence, and foreign intelligence sharing.
- **Department of Defense** is responsible for deterring, defending against, and defeating aviation threats to the United States and its global interests; airborne response and resolution of nation-state threats within the ATS; and the operational response to actual or potential airborne threats in U.S. airspace or the air approaches to the United States until the threat has either been resolved or defeated.
- **Department of State** is responsible for coordinating U.S. Government initiatives that involve foreign governments and international organizations, including regional aviation security cooperation.
- **Department of Commerce (DOC)** is responsible for providing aviation industry and trade policy expertise in both inter-agency policy efforts and international negotiations.

Federal departments and agencies represent a segment of the aviation mode. The large volume of cargo and number of passengers flying into the United States from overseas via aviation assets increases the importance of strong partnerships at the Federal level with international and domestic aviation partners. Foreign governments, State and local law enforcement, and passengers play key roles in the multi-layered protective posture that has significantly enhanced aviation security from where it stood on September 11, 2001. These collaborative partnerships are integral in ensuring the safety, protection, and prosperity of the individuals, businesses, and organizations that rely on the ATS every day.

2.3.2 Aviation Modal Partnership Framework

The Transportation Systems Sector-Specific Plan (SSP) describes the sector's partnership model, which provides a collaborative mechanism for the development of processes, policies, plans, and reports for the protection and resiliency of critical transportation infrastructure, passengers, and cargo. The ATS applies the sector's partnership model, and other means, to incorporate the views of a wide range of public and private partners in its policy determinations. Specifically, several committees were formed under the Critical Infrastructure Partnership Advisory Committee (CIPAC) to focus on protecting critical aviation infrastructure in the Transportation Systems Sector. These include the:

- Aviation Government Coordinating Council (AGCC): composed of representatives of government agencies, including: TSA, FAA, the DHS Office of Infrastructure Protection (IP), the Federal Bureau of Investigation (FBI), DoD, and the National Association of State Airline Officials (designated State government officials).
- Aviation Sector Coordinating Council (ASCC): composed of representatives of the owners and operators of critical transportation infrastructure including: Aerospace Industries Association; Air Transport Association; Air Carrier Association of America; Airport Consultants Council; Airports Council International – North America; American Association of Airport Executives; Aircraft Owners and Pilots Association; National Air Carrier Association; National Business Aviation Association, Incorporated; and Regional Airline Association.

In addition to the ASCC and AGCC, which were established under the CIPAC framework, partner engagement within the aviation mode is bolstered through the Aviation Security Advisory Committee (ASAC). The ASAC was formed under the authority of the Federal Advisory Committee Act to permit non-Federal entities to advise the Federal Government about aviation security policies and practices in an open and transparent forum. ASAC membership is comprised of representatives of aviation modal owners and operators, labor organizations, and the general public.

Internationally, several Federal departments and agencies represent the United States in numerous multilateral venues in order to achieve our homeland security objectives and to harmonize security standards. These forums help to standardize national aviation security efforts to collectively improve the mode's global risk profile.

National and global situational awareness has improved through collaboration among aviation modal partners, including U.S. and foreign governments. This has been achieved through tools that integrate intelligence, surveillance, reconnaissance, flight and other aeronautical data, navigation systems, and other operational information. To ensure effective and coordinated action, domain awareness information must be available at the appropriate classification level to agencies across the U.S. Government, local government, industry partners, and the international community. Aviation modal partners continue to enhance the capabilities of current information systems and to develop new capabilities and procedures that locate and track aviation threats and illicit activities. These efforts are integral to the risk mitigation strategy within the ATS.

2.4 Risk Management

Risk management has increased in importance throughout the ATS over the years. As a result, changes have been made to develop risk-informed, decisionmaking approaches to determine the programs and processes necessary to achieve the aviation mode's goals and objectives (explained in more detail in section 3.1). Achieving these goals and objectives relies heavily on the continued partnership between government and industry, with a clear focus on implementing efficient and effective risk mitigating measures.

2.4.1 Risk Profile

The security and economic prosperity of the United States depend significantly upon the secure operation of its ATS and safe use of the world's airspace. The vast number of daily aviation operations worldwide that involve U.S. assets creates an attractive target for terrorists. Terrorists, criminals, and hostile nation-states have long viewed the ATS as a target for attack and

exploitation. However, the risk profile of the ATS is constantly changing, and risk mitigation efforts evolve simultaneously. Aviation modal partners utilize timely information-sharing products in order to continually reevaluate countermeasures to ensure that risks are thoroughly and efficiently managed.

A significant threat to the ATS, and a central focus of Federal aviation security efforts, is the potential for terrorist infiltrations and attacks. The United States faces an enduring, complex, and adaptive enemy, and it is incumbent upon the Federal Government and other aviation stakeholders to remain vigilant in dealing with this threat.

The ATS is a global enterprise with distributed infrastructure and multiple access points. These characteristics have enabled the system to quickly achieve a global reach, with ease, to users around the world. These same characteristics, however, also enable terrorists to achieve mass casualties and significant economic damage via attacks on or using the ATS.

The aviation mode has also focused on developing countermeasures to address specific risks in the cyber realm. Cyber systems are an integral part of the aviation mode, contributing to the efficient operation of the NAS, airport and air cargo facilities, and airline systems. As noted in the NSAS and its seven supporting plans, DHS, DOT, and DoD continue to develop and enhance technological and procedural measures to detect, prevent, respond to, and recover from physical and cyber-based attacks on the ATS's critical infrastructure. A concerted, well-orchestrated attack on any modal cyber network could cause considerable disruption mode-wide, on both the national and international scales. This criticality necessitates the inclusion of cyber threats, vulnerabilities, and consequences in the overall analysis of day-to-day sector risk.

Threats focused on the ATS can be analyzed in two broad categories: by originator and by targets and tactics. There are two main originators of threats: terrorist groups and common criminals.

Terrorist Groups. The terrorist threat to the ATS has morphed over the years as intentions and capabilities of individual terrorists and their affiliated organizations, in some cases change. Terrorist groups are adapting to aviation countermeasures in multiple ways, including modality of planning, complexity of potential attacks, and methods of attack execution.

One difficulty in countering terrorist threats to the ATS is that terrorists may use the same tactics, techniques, and methods pioneered by common criminals. These tactics enable terrorists to counter immigration, customs, and border security measures to move people and material in order to execute an attack. They may deploy in regions of political and economic instability where aviation law enforcement is stretched thin or readily corruptible. They may be able to bribe officials, use forged fraudulent documents, and/or make illegal transactions to hide their true intentions. Terrorists may use unsecured air transportation routes to transport arms, explosives, or operatives clandestinely to safe havens, training sites, or attack-staging locations. Ultimately, terrorists may use these access points and routes to transport more dangerous cargo, including weapons of mass destruction (WMDs) and their associated components.

Criminals. Criminals, including individuals and groups, use the ATS to pursue objectives that are illegal under U.S. law or international convention. These include potentially violent domestic groups and individuals who have both extensive knowledge of aviation assets, systems, and networks and a demonstrated expertise in manufacturing and employing targeted-attack techniques, including improvised explosive devices (IEDs). While the motives of criminals differ from those of terrorists, other aspects of their operations are sufficiently similar that many countermeasures will be effective against both.

2.4.2 Aviation Threat Categories

There are three primary categories of threats to the ATS arising from both criminal and terrorist actors:

- Aircraft as a target and/or weapon,
- ATS infrastructure as a target, and
- Hostile exploitation of cargo.

Threats to and from Aircraft. Several categories of aircraft are susceptible to being attacked, or to being used to attack other targets. Historically, large passenger aircraft have been at greatest risk of attack because adversaries perceive such aircraft as having great potential to inflict catastrophic damage and such an attack as being likely to disrupt the ATS. Aircraft have been the primary target of attacks in the past, and have used as weapons, with the intention of disrupting American prosperity and freedom. Terrorists may also attempt to use large all-cargo aircraft as weapons to attack ground-based targets.

Similarly, terrorists may use small aircraft as weapons to attack other targets. Due to their size, small aircraft are relatively unattractive as targets, but certain types of aircraft, in particular fast general aviation aircraft with trans-continental range, may be of interest to terrorists planning on attacking critical infrastructure. Additionally, transnational criminal elements employ small aircraft to conduct illicit activities in the ATS, including smuggling people and contraband.

Threats to ATS Infrastructure. Reported threats to ATS infrastructure are few in number. In part, this is due to the relatively low public profile of ATS infrastructure, the robustness and resilience of these systems, and the Nation's capacity to recover rapidly from an attack thus limiting the psychological or economic impact of an attack.

Terrorists could target passengers, as well as the infrastructures at airports, by placing explosives near or inside passenger facilities. Such a technique may be particularly effective at multi-use airports, such as those combining commercial and military operations or commercial and general aviation operations, where unrelated security authorities and dissimilar security procedures co-exist. A Vehicle-Borne Improvised Explosive Device (VBIED) was used in the 2007 attack at the Glasgow International Airport and in the 2010 attempted attack by Faisal Shahzad in Times Square, New York City. VBIEDs remain a viable, destructive, and lethal means of targeting ATS infrastructure. In 2007, New York Police thwarted a plot to attack a fuel storage and pipeline infrastructure serving John F. Kennedy Airport.

The aviation mode has also focused on specific risks in the cyber realm. Cyber systems are an integral part of the ATS, contributing to the efficient operation of the NAS, airport and air cargo facilities, and airline systems. A concerted, well-orchestrated attack on any modal cyber network could cause considerable disruption, mode-wide, on both the national and international scales. This criticality necessitates the inclusion of cyber threats, vulnerabilities, and consequences in the overall analysis of modal risk.

Threats from the Hostile Exploitation of Cargo. The air-cargo industry is highly dynamic and encompasses a wide range of users; characteristics which expose it to exploitation by terrorists. Many users, ranging from express consignment carriers that operate complex sorting operations at major hubs for time-definite cargo delivery to small regional carriers that move high-value cargo or service rural areas, are highly regulated. Enhanced security measures have reduced both the risk of stowaways and the introduction of explosives into cargo; however, cargo systems remain vulnerable to exploitation.

The attacks of September 11, 2001, the Heathrow liquid explosives plot of August 2006, and the December 25, 2009 terrorist incident on Northwest flight 253 are reminders of the threats facing aviation and the malicious intent of adversaries. These events have significantly elevated the level of public concern for securing and protecting the ATS.

2.4.3 Aviation Modal Risk Assessment Process

Security risk in the ATS, as throughout the Transportation Systems Sector, is a function of threat, vulnerability, and consequence (See chapter 3 of the SSP Base Plan). A risk assessment is a product or process which collects and evaluates information and intelligence, and yields a risk score to inform priorities, develop or compare courses of action, and inform risk-based decisionmaking. To evaluate risk across the modes, the sector uses a process (as detailed in chapter 4 of the SSP Base Plan) which engages collaborative teams of government and private sector risk management professionals and security experts from each transportation mode. The Transportation Systems Sector Security Risk Assessment (TSSRA), completed in early 2010, leveraged the specialized experiences and backgrounds of experts, in conjunction with results and findings from risk methodologies and assessments throughout DHS. The TSSRA method employs an analytical framework with rigorously applied business processes

to facilitate transparent, defensible comparisons across the modes of transportation. However, aspects of the TSSRA were tailored for specific modes, including aviation, and adapted critical details to the risk profiles of each.

Within the TSSRA framework, the Aviation Modal Risk Assessment (AMRA) incorporates relevant threat, vulnerability, and consequence data to prioritize risks unique to the aviation mode. In conducting the AMRA, the values for these factors are determined by risk management professionals and security partners throughout the ATS. Given the continually evolving nature of the threats, hundreds of risk-based scenarios are used in the AMRA process. These threat scenarios are based on historical terrorist events and current intelligence streams to ensure relevancy and accuracy.

Once developed, the scenarios provide a framework for estimating the human, economic, physical, and psychological impacts of an incident. These are a function of unresolved vulnerabilities, and provide a consequence score for each scenario. The combined threats, vulnerabilities, and consequences inform the protection priorities and risk mitigation efforts that the mode must consider. Priorities and resources can be more effectively aligned with relevant and timely risk assessment information.

2.4.4 Risk Management Analysis Process

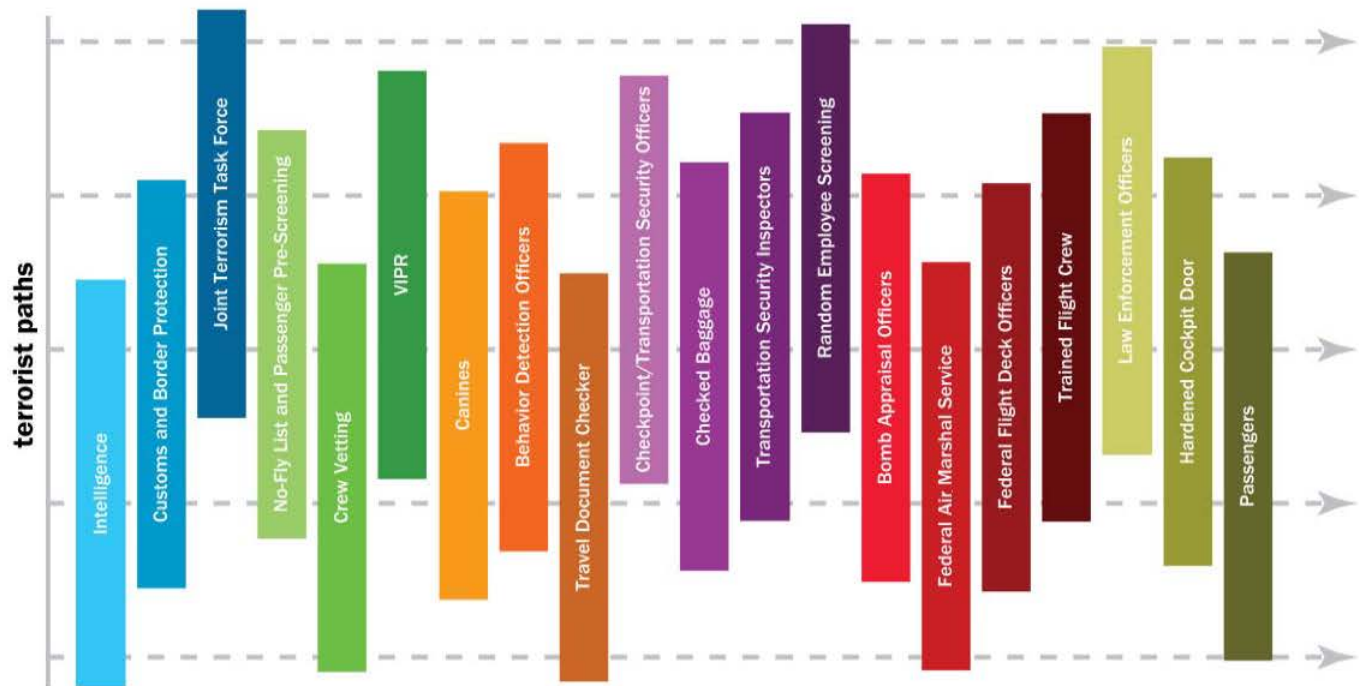
TSA has also partnered with industry to create the Risk Management Analysis Process (RMAP), an innovative risk evaluation method that uses an agent-based, Monte Carlo simulation model to provide insights for security countermeasure investment decisions. RMAP supports the aviation mode by using subject matter expertise to produce insights on risk reduction and economic impacts associated with implementing countermeasures. RMAP addresses the high degrees of complexity and uncertainty, the continuous adaptation of the adversary, and the dynamics of individual risks. Additionally, RMAP provides sector leadership the ability to assess changes to risk, analyze countermeasures, and prioritize and evaluate alternatives to make risk-informed decisions. RMAP also fulfills the requirement for TSA to have a structured risk-informed decisionmaking process, as stipulated by the U.S. Government Accountability Office (GAO), Congress, and DHS.

2.4.5 Risk Mitigation Strategy

In order to improve the protection and resiliency of aviation infrastructure, the mode applies a layered approach to risk reduction programming. This layered strategy features risk mitigation activities that address vulnerabilities by involving multiple jurisdictions, overlapping technologies and processes, and increasing surveillance and screening on approach to critical nodes in the ATS. The coordinated participation of government authorities and private sector security personnel in infrastructure protection and emergency response provides the multi-jurisdictional layering deemed essential to efficient risk management. Ultimately, the effectiveness of this layered risk mitigation strategy is also enhanced by an alert, aware, and informed traveling public.

During risk assessments, vulnerabilities are identified and analyzed to determine if programs should be developed to reduce those vulnerabilities, and thereby reduce the overall risk. For example, a security awareness vulnerability might be addressed through a set of layered training initiatives including entry level, front-line, and security force training conducted through online, classroom, and exercise venues. A broad range of programs and initiatives ensures that risk mitigation efforts are comprehensive and adaptive to the constantly changing risk profile. A notional map of the layering approach in the aviation mode is depicted in figure A2-2.

Figure A2-1: Layered Approach to Aviation Security



The specific programs and processes developed to mitigate identified risks in the ATS are further explored in section 3 in order to achieve the aviation mode's goals and objectives.



3. Implementation Plan

3.1 Goals, Objectives, and Programs/Processes

The Transportation Systems SSP process for identifying sector goals reflects the collaborative approach of the entire SSP development process, as directed by HSPD-7. The Transportation Systems Sector goals presented in the Base Plan represent the consensus of the sector's partners. To achieve long-term success in securing the Aviation Transportation System, the sector goals will need to be seamlessly integrated into a risk-informed decisionmaking framework. The following programs are used to illustrate how the goals and objectives in the Aviation Transportation System are being met. This section does not represent a comprehensive list of programs and processes, and many programs may fulfill multiple goals and objectives. Appendix 1 to this plan lists some of the key aviation programs.

3.1.1 Goal 1: Prevent and Deter Acts of Terrorism Using or Against the Transportation System

Objectives

- Implement flexible, layered, and unpredictable security programs using risk management principles.
- Increase the vigilance of travelers and transportation workers.

The Federal Government, in cooperation with its modal partners, continues to work within the changing threat environment to identify and mitigate potential threats and risks to the ATS. At the heart of this challenging endeavor is a comprehensive strategy based on risk management principles. This strategy blends and layers complementary elements such as innovative programs, emerging technologies, and operational practices, including unpredictable deterrents, that are flexible and adaptive to the constantly changing environment. Aviation modal partners will continue building on their successes in implementing this strategy, while augmenting it with cross-modal outreach efforts aimed at increasing the vigilance of travelers and transportation workers, therefore leveraging them as force multipliers. Outreach, in cooperation and coordination with FAA, DoD, DOJ, and key modal partners, is a key factor in maintaining vigilant domain awareness to protect the United States from threats in the aviation domain.

Risk Management

The aviation mode risk management approach applies the principles in the Base Plan to systems-based and asset-based risks and serves as the foundation of the implementation plan. The approach builds on the aviation risk profile, develops the standards and criteria for a common, relevant operational picture to aid stakeholders to make effective decisions, and generates a portfolio of alternative management strategies that reduce aviation vulnerabilities and improve system resiliency. Risk management includes key factors in the decisionmaking environment, such as executive, legislative, budgetary, and industry concerns, and serves to inform the prioritization process, so that threats can be effectively managed.

Operational Practices

Aviation modal partners will continue to enhance aviation security through intelligence-driven and risk-based operations, programs, processes, and procedures that are flexible, layered, and unpredictable to deter, prevent, and detect threats. Such successful programs as the random deployment of VIPR Teams at airports, Federal Air Marshals (FAMs) onboard flights, and Federal Flight Deck Officers (FFDOs) in cockpits augment the deterrents served by passenger and baggage screening conducted by Transportation Security Officers (TSOs) and canine teams. The implementation of programs such as Security Evolution and Playbook reflects a strategic shift from operations based on Standard Operating Procedures and concentrating on objects to an intelligence-based, risk-driven approach that emphasizes anticipating and recognizing anomalous behavior, situations, and objects through skilled human engagement.

To adapt to the ever-changing threat environment, aviation modal partners will continue to expand these programs through increased deployments, enhanced detection and awareness skills, and the leveraging of technologies. Additionally, a Federal initiative seeks to increase the presence of armed law enforcement officers and canine teams at airport screening checkpoints. These teams will work with Federal, State, local, and tribal security and law enforcement officials to supplement existing security resources and provide deterrent presence and detection capabilities. Federal, State, and local Law Enforcement Officers Flying Armed (LEOFA) serve as force multipliers. All officers who fly armed are required to take a LEOFA training course. The increased and consolidated law enforcement presence will enhance prevention, protection, and response capabilities across critical aviation physical infrastructure and foster closer collaboration among law enforcement agencies.

One of the most significant layers of security stems from an Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act) requirement to screen 100 percent of cargo on passenger aircraft. The implementation of the Certified Cargo Screening Program (CCSP), a voluntary, facilities-based program, will continue to enhance the resiliency of cargo movement along several nodes of the supply chain. TSA works collaboratively with private industry to minimize the impacts of cargo screening requirements on passenger air travel and stakeholders. As standard security programs to support the CCSP are implemented, more Certified Cargo Screening Facilities (CCSFs) along the supply chain will be created. Mandated inspections and oversight of CCSFs allow the mode to decrease the threat of explosives being introduced into cargo.

Traveler and transportation worker vetting programs are another important component in reducing terrorism risks. Aviation modal partners have long recognized the safety and security role of vetting workers' backgrounds and are working to modernize and consolidate the information technology infrastructure for enrollment, vetting, and credentialing services. Providing LEOs and aviation personnel with biometric cards and the associated technologies that work with the vetting programs would serve to strengthen identification and access control to critical infrastructure of the ATS. Furthermore, recognizing that exploitation of trusted positions and information could jeopardize security, the Insider Threat Mitigation Program will identify and resolve illegal activities or crimes perpetrated from within the transportation workforce.

Passenger vetting through TSA's Secure Flight and CBP's Advance Passenger Information System (APIS) significantly enhance the security of domestic and international commercial air travel through the use of improved watch list matching. These programs support the goal by conducting uniform prescreening of passenger information against Federal Government watch lists for domestic and international flights into, out of, within, and over the United States. To promote efficient passenger vetting and minimize unnecessary inconveniences to the traveling public, TSA relies on the assistance of aviation modal partners to review the criteria for terrorist watch lists and to enhance the Transportation Security Redress programs. This will streamline traveler vetting by increasing accuracy of positive hits and decreasing misidentified travelers.

Outreach

Another important component of the strategy is keeping aviation workers, stakeholders, and the public aware of security efforts through the use of programs like the GA Secure Hotline and the Air Cargo Watch Program, that directly support the objective of increasing the vigilance of travelers and transportation workers. The ATS will continue its GA Secure Hotline as a centralized

reporting system. The GA Secure Hotline is designed to educate GA airport managers, users, tenants and aircraft owners/operators on security measures, best recommended security practices, as well as provide a single government entity to report suspicious and security related activities. The ATS and private industry partners will continue to develop marketing and promotional materials that will be distributed to 650,000 general aviation airport and aircraft operators, including pilot groups and individual pilots. These outreach activities include stakeholder information sharing and public announcements within the ATS and other means of communicating to the public how to prevent a security incident and how to respond should an event occur. An example of such an activity is the “If You See Something, Say Something” campaign that empowers travelers to become force multipliers to keep travelers safe. Increasing awareness and vigilance of both travelers and transportation workers allows for additional layers of security to deter and detect threats to aviation assets, systems, and networks.

3.1.2 Goal 2: Enhance the All-Hazard Preparedness and Resilience of the Aviation Transportation System to Safeguard U.S. National Interests

Objectives

- Continually identify and assess critical aviation infrastructure using the risk management framework.
- Analyze infrastructure assessments and focus efforts to mitigate risks and to improve overall network survivability.
- Identify capacity or technology gaps in protection and prevention response capabilities necessary for the expeditious recovery of critical systems.
- Develop aviation modal processes to determine critical cyber assets, systems, and networks and to identify and implement measures to address strategic cybersecurity priorities.

To continue to improve the Aviation Transportation System’s comprehensive risk posture, TSA, FAA, and other Federal aviation modal partners will continue to focus on activities that not only manage risk, but also enhance resilience in the system, including activities focused on prevention, preparedness, and the ability of the network to recover quickly from an incident. Building preparedness and ensuring resilience in the ATS rests on using a risk management approach to identify network vulnerabilities, leveraging the results of risk management activities to identify capability or technology gaps, and developing security plans to address any identified gaps. Security planning should be aligned across the ATS to effectively create an integrated, synergistic, system-wide strategy.

Risk Management

TSA, FAA, and other Federal aviation modal partners have developed and implemented a comprehensive risk management framework. Risk management tools comprise an important component of such an approach. For example, the primary security risk management tool used in TSA is AMRA, formerly referred to as the Air Domain Risk Assessment. AMRA’s baseline risk assessment includes both domestic and international aviation assets, systems, and networks. As described in section 2.4.2, AMRA is the aviation component of TSSRA, the comprehensive cross-modal assessment that uses a scenario-based assessment of the threats, vulnerabilities, and consequences associated with each mode of transportation, as well as an integrated look across all the modes of transportation. AMRA meets the requirements of specific risk actions for the National Strategy for Aviation Security (NSAS), specifically action items of the Air Domain Surveillance and Intelligence Integration (ADSII) and the Aviation Transportation System Security (ATSS).

TSA will leverage AMRA to continue developing the qualitative and quantitative approaches to mitigate risks and improve overall network survivability. As the primary tool used to assess and rank risks, AMRA uses risk assessments to provide descriptions of the risk-based priorities for securing threats. Identifying and prioritizing the greatest aviation security needs will help inform the allocation of resources within the ATS.

Moreover, key components of the ATS are complemented by redundant systems, reserve capacity, and traffic routing alternatives that provide significant system resiliency in the present state. Compliance and assessments, both voluntary and required, are an important component of measuring system resiliency to security threats. Explained more in section 3.2.3, these processes are conducted by TSA and FAA inspectors domestically and internationally. One comprehensive site assessment conducted by DHS with DOE participation reviews control systems throughout the critical sectors, including within the ATS. In this process, subject matter experts evaluate current risk mitigation practices, assess relevant threats, and recommend operational changes at facilities to enhance risk management efforts. This program is continually expanding its private sector exposure to engage with a wide range of private and industry aviation modal partners. The cumulative results of these assessments, surveys, and inspections yield more specific information about risk mitigating activities to determine the effectiveness of ongoing initiatives or to identify gaps in protection and resiliency targets.

Gap Analysis

Aviation protection initiatives are derived from formal or informal assessments of threats and risks to the ATS. These assessments enable the mode's security and protection officials to identify shortcomings or gaps in current protective measures or gaps where needed capabilities are not in place. These vulnerability and capability gaps describe shortfalls in equipment, processes, procedures, or technologies that are deemed necessary to counter threats, enhance protection and resilience, and facilitate recovery.

TSA, its security partners, and the IC continuously monitor intelligence for patterns, trends, indications, and warnings of threats to the ATS. Threat information and vulnerability assessments are analyzed to understand how the threats might be successful given the type of countermeasures in place and their effectiveness. TSA will use a newly developed simulation model, the Risk Management Analysis Tool (RMAT), to evaluate risks in airports. The tool will allow different threat scenarios and existing or proposed countermeasures to be evaluated. While the tool's primary purpose is to analyze effectiveness of proposed countermeasures, it also may be used to identify vulnerabilities where more detailed analysis is indicated.

Terrorists seek ways to thwart security measures and to exploit weaknesses or gaps in the layers of aviation security. Vulnerabilities might be related to the absence of, or the ineffective functioning of, a protection program or to the lack of a technological capability. TSA and DHS conduct covert testing of airport security operations to identify vulnerabilities in procedures, detection capabilities, and training. TSA, the FAA, and other protection partners also assess gaps through several other approaches such as formal and informal gaming methods, "red teaming," and exercises. For example, DHS and the Department of Health and Human Services conducted a series of exercises, including a full-scale mock-up exercise, at selected airports to train for and test health screening procedures in the event of a pandemic outbreak outside United States. The results allowed analysis of such integral issues as outreach and communication to non-English speaking communities and proper planning for at-risk populations.

Vulnerabilities attributed to the lack of technology capabilities, such as vetting and credentialing capabilities, are evaluated through TSA's Capability Gap Process and refined for consideration through a deliberative project development, prioritization, and resourcing process managed by the DHS Office of Science and Technology.

Planning

Protecting the security of the American people is a continuing commitment that requires wide-ranging planning to address security challenges. The better prepared the ATS is in advance, the better it can respond to crises, whether they are terrorism or manmade. A planning system is an evolutionary process that is able to transform strategic guidance and policies into strategic, operational, and tactical plans. This effort requires a planning capability, which consists of planners, processes, and procedures to address multi-faceted challenges across the spectrum of operations in preparation for effectively preventing, responding to, and recovering from incidents.

TSA achieves this capability through deliberate planning activities. TSA has developed and implemented the Incident Management Framework which is consistent with guidance derived from the National Incident Management System and the National Response Framework (NRF), as updated in 2008. The Incident Management Framework establishes TSA incident management operations and the concepts, principles, plans and specific procedures that provide for a rapid and effective TSA response to any incident or threat affecting the Nation's transportation sector, or in support of a broader effort under the NRF. TSA coordinates high-profile special events and ensures all activities are fully coordinated with DHS, Federal Emergency Management Agency, and other Federal agencies.

The National Preparedness Guidelines describe a coordinated approach to all-hazard incident management planning across Federal, State, local, tribal, territorial, and private sector entities; however, aviation modal partners have historically developed contingency plans independently. While exercises help to achieve unity of effort among aviation modal partners, more deliberate activities should be explored to develop integrated planning processes that include all jurisdictional levels of government and private industry to enhance system resiliency.

Cybersecurity

Cyber systems, including air traffic control, tracking, and communication systems needed to support commerce, provide a fundamental capability in keeping the Nation's transportation system safe and operational, especially given growing foreign dependencies. The cybersecurity objectives for the mode are to understand the risks associated with the cyber component of critical infrastructure within the ATS, to share that information with aviation partners as a part of the overall risk management and decisionmaking process, and to develop countermeasures and programs to address the growing threats. Additional responsibilities include, but are not limited to, identifying best practices and standards across the mode and in other sectors, sharing threat vector data with partners, and supporting the development of cyber metrics.

Federal agencies must meet Federal Information Security Management Act requirements to secure cyber systems from internal and external threats. These initiatives include protecting Federal-private information-sharing linkages. Cybersecurity in the aviation industry is the responsibility of individual aviation service providers. A collaborative effort involving aviation protection partners has been engaged through the Transportation Systems Sector's Cybersecurity Working Group (TSS CWG). In order to achieve this objective, the working group is implementing the risk management framework to identify cyber risks, prioritize those risks, develop protection solutions and architectures to mitigate those risks, and build a governance process to assure those mitigations are correct and that new risks are continually addressed.

Specific actions in the NSAS require the development of technological and procedural measures to address cybersecurity attacks. DHS, DoD, and DOT are conducting a comprehensive risk assessment and are developing a research, development, testing, and evaluation program to address cyber, radio frequency, and electromagnetic pulse attacks. These interagency activities will align with FAA's Joint Planning and Development Office (JPDO) Next Generation (NextGen) Air Transportation System (NGATS) enterprise architecture and concept of operations. By maintaining alignment, DOT, DHS, and DoD jointly ensure a cost effective and consistent evolution and implementation path of these aviation security programs.

Other actions in NSAS involve the development of additional security measures in the NAS infrastructure. Security incident reporting and response is managed at the FAA enterprise level by the FAA Cyber Security Incident Response Center and within the Air Traffic Organization by the Security Information Group. The latter organization provides real-time NAS cybersecurity risk management capability through event and intelligence fusion. These procedures are essential to ensuring a secure operating environment within the aviation community.

Federal aviation partners also work closely with the DHS National Cyber Security Division (NCSD) to continually evaluate cyber risks to the mode. Specifically, TSA and FAA participate in the Cross-Sector Cyber Security Working Group (CSCSWG), whose membership includes a wide variety of Federal, State, local government, and private sector cybersecurity experts. This working

group facilitates the sharing of information on best practices, lessons learned, common vulnerabilities, prevailing threats, and mitigation strategies across sectors.

3.1.3 Goal 3: Improve the Effective Use of Resources for Transportation Security

Objectives

- Align aviation modal resources with the highest priority protection and resiliency needs using both risk and economic analyses as decision criteria.
- Promote aviation modal participation in the development and implementation of public sector programs for asset, system, and network protection.
- Ensure coordination and enhance risk-based prioritization of aviation security research, development, test, and evaluation (RDT&E) efforts.
- Coordinate policy and minimize duplication of efforts by Federal, State, and local government agencies to improve aviation safety and security.

Protecting the expansive Aviation Transportation System is a complex endeavor that requires many trade-offs among finite resources. The aviation system's partners must therefore continually ensure that resources are adequately allocated and efficiently utilized. Therefore, improving the effective use of resources is a key component of the implementation plan. Aligning resources in an effective and efficient manner will be accomplished through a comprehensive approach, leveraging performance management that uses both risk and economic analyses, coordinates among modal partners and government agencies, and significantly enhances research and development efforts. Criteria for selecting critical assets, networks, and systems continue to evolve and improve to define the scope of risk management activities within the ATS. Critical aviation infrastructure identified through the risk management process is prioritized to allocate resources effectively throughout the ATS.

Performance Management

Performance management—with respect to risk-reduction activities for all types of hazards—involves the ability to assess the collective impacts of the protection and resiliency activities of all aviation modal partners including our international partners. The Federal modal partners, TSA and FAA in particular, have extensive measurement initiatives to provide agency-specific data about program implementation, operations, and effectiveness that inform management decisions within the administration and in Congress. Process efficiencies are advocated through such programs as DHS Travelers Redress Inquiry Program, which allows for streamlined traveler vetting, improved watch list matching, and decreased passenger inconveniences. The industry provides substantial data regarding its operations to the Federal Government, as required by regulations, regarding operations, airmen testing, accidents, passenger manifests and behavior, cargo information, grants data, safety, and security.

In addition, the modal partners jointly participate in aviation risk assessments that evaluate hundreds of possible threat scenarios to aviation infrastructure. Information collected during compliance inspections, security assessments, and surveys provides additional information for analysis of protection and resiliency program performance. The objective is to support program metrics which indicate progress reducing risks related to vulnerabilities or gaps that have been determined to be unacceptable. A sector objective is to develop a common dataset for assessments, compliance inspections, and surveys that will provide greater opportunity for expanded analyses and cross-modal comparisons.

As a part of the performance management approach, TSA and FAA continue to evaluate compliance with aviation safety and security policies, programs, and regulations through a cadre of specialized inspectors. While TSA Aviation Security Inspectors and FAA Aviation Safety Inspectors conduct field inspections, TSA Principal Security Specialists (PSSs) conduct corporate-level review of security programs and practices for general aviation, commercial airlines, and cargo carriers, including aspects of crew defense training. PSSs provide technical review and analysis in the development, coordination, and issuance of national

policies, standards, and procedures governing aviation security with emphasis on domestic, international cargo, and passenger aircraft operator security. These inspection and assessment activities are an important element of performance assessment and management in the airline carrier and airport communities.

The mode provides annual performance reports on its protection and resiliency program activities to DHS under risk mitigation activity (RMA) categories. A full discussion of the RMAs may be found in chapter 5 of the SSP Base Plan. Typically several representative programs or initiatives are included in a RMA category. For example, the RMA “Risk-mitigating Operational Practices,” includes the National Explosives Detection Canine Team (NEDCT) program, the SPOT program, and the CCSP. The goal of the SPOT program is to identify potentially high-risk passengers through non-intrusive behavior observation and analysis techniques. Specially trained Behavioral Detection Officers (BDOs) are deployed at strategic locations to observe people within the aviation properties and, if appropriate, to refer those persons raising suspicion to law enforcement offices. Performance is assessed relative to the number of referrals with positive results. Another activity in this RMA category is the Certified Cargo Screening Program (CCSP). CCSP promotes sector participation in the development and implementation of public sector programs intended to reduce risks within aviation related to air cargo. The initiative enables air cargo to be screened at various nodes of the supply chain, including certified shippers and indirect air carriers. Cargo screened under this program arrives at the air carriers ready for up-loading, thus facilitating the efficient flow of commerce. The 9/11 Act requires performance standard of 100 percent screening of cargo on passenger flights by August 2010. TSA will monitor the performance of this program through data collection and audits. Lastly, the Electronic Boarding Pass Program is another program within this RMA. The goal of this program is to enhance efficiency and minimize passenger delays. Performance is monitored based on measures of the specific aspects of the boarding process to minimize the duplication of efforts, improve coordination, and align resources to address the highest risks.

Research and Development

An integral component in risk management mentioned in the gap analysis process is research and development (R&D) of technologies. Ongoing challenges to sector R&D efforts include the diversity of ownership of aviation assets, the inherent vulnerability of aviation transportation, the constant evolution of security, and the increasing dependency on intermodal and international transportation. For these reasons, continual involvement by the private sector and aviation security partners is paramount to successfully addressing these challenges. Since R&D is a shared activity across the Federal Government and private sector, there is a great deal of insight to harness that will help in developing appropriate technology requirements. The Transportation Systems Sector R&D Working Group brings these stakeholders together from across the mode to identify mission needs and capability gaps. From these requirements, development efforts are derived, often including identification of short-, medium-, and long-term desired outcomes. These needs and gaps are eventually forwarded into the DHS S&T Capstone Integrated Project Team Process, which allows multiple Federal partners to collaborate to develop programs and projects that close capability gaps and expand related mission competencies. In the SSP Base Plan, chapter 7 provides a more detailed description of R&D processes.

R&D activities are funded through the grants process or other vehicles to influence the design of new capabilities. R&D inputs to requirements are also driven by the evolution of technology capabilities. The continual scanning of current and new technological advances across the government, private sector, and academia enables greater potential deployment of technology-enabled solutions for enhanced security at the same or lesser cost than existing protection measures. It also reveals the potential for new security capabilities not previously considered. These benefits underscore the continual and critical importance of aviation modal partner engagement in R&D efforts.

R&D initiatives, ATS goals, and other guidance from aviation modal partners influence the assessment and prioritization of mitigation options. Risk-based sector technology requirements seek to enhance screening effectiveness for passengers, baggage, cargo, and materials for aviation, enhance infrastructure and conveyance security, improve information gathering and analy-

sis, provide a common operating picture for transportation systems, and implement needed cybersecurity capabilities. These programs may then result in pilot test programs, followed by deployment or testing in the field.

Following this approach, the Federal Government will continue introducing new pilot programs, if and when appropriate, that integrate and coordinate various measures. For example, a significant effort has been undertaken in the development the NGATS and the Flight Data Initiative (FDI). These projects will enable both a near and future-state of Air Domain Awareness. NextGen is a transformation of the NAS, including the national system of airports, using 21st century technologies to ensure future safety, capacity and environmental needs are met. NextGen will leverage state-of-the-art technology to identify new airport infrastructure and new procedures, including the shifting of certain decisionmaking responsibility from the ground to the cockpit. FDI solutions will enhance safety and address a gap in the layered security strategy by capturing real-time activities of in-flight commercial aircraft and thus augment incident management capabilities. FDI also complements the core missions of FAA, TSA, and the National Transportation Safety Board (NTSB).

Other examples of R&D initiatives include the recent electronic boarding pass pilot that enables passengers to download their boarding pass with encrypted two-dimensional bar code along with passenger and flight information onto their cell phones or personal digital assistants, which TSOs can validate with hand-held scanners. This innovative approach streamlines the customer experience while heightening the ability to detect fraudulent boarding passes. Pilot programs in air cargo screening, such as the research, development, testing, evaluation, and subsequent deployment of Advanced Technology X-ray and Explosive Detection Systems, are designed to identify innovative methods to protect the integrity of air cargo from the time of acceptance until tendering at the airport. Pilot programs will also evaluate tamper-evident and tamper-resistant seals and locks to secure air cargo in transit. Personnel selection tools, cargo-specific training programs, and training aids, such as threat image projection that can superimpose stored images of threat objects in scanned images of cargo items, are used to improve the human operator performance of the air cargo inspection system.

Aviation Partnerships

Aviation security partners seek to achieve greater efficiencies and economies through expanded efforts to reduce duplication of compliance and assessment activities, to consolidate safety and security program objectives where possible, and to seek greater collaboration with aviation industry and the traveling public. Constant collaboration with government and private industry security partners is an integral component of the iterative risk management processes. This allows Federal, State, and local government agencies to effectively coordinate to maximize R&D initiatives, coordinate policy, and minimize duplication of efforts to improve aviation security while ensuring the efficient use of limited resources.

The ATS has several formal and informal channels in which protection and resiliency programs are reviewed to ensure policies are coordinated, various perspectives are analyzed, and duplication of effort is minimized. Some groups are convened to study specific needs such as protocols for handling communicable diseases or the security gaps circumvented by specific threat incidents. Working groups, such as the Aviation Security Working Group and the Air Domain Awareness Working Group, advance broad strategic and policy initiatives. The private sector provides advice to government agencies through the ASAC, the AGCC, and the ASCC. Several CIPAC-approved joint cross-sector working groups provide opportunity for participants to contribute to the development of cybersecurity and R&D initiatives. The private sector and the general public also have an opportunity to comment on regulatory initiatives announced in the Federal Register through the Notice of Proposed Rulemaking process.

The One DHS Solution was created through a collaborative effort among Federal partners to support airlines by developing unified requirements for the Customs and Border Protection (CBP) APIS and TSA Secure Flight. TSA and CBP collaborated in other programs and systems, such as the Airspace Waiver Program and Automatic Detection and Processing Terminal (ADAPT) program. Improved interagency coordination could result in the approval of new international flight routes.

Aviation model partners continue to work closely with foreign governments to leverage existing aviation security practices and to work towards compatibility across systems to the greatest extent possible. Aviation security partners have been working in

both bilateral and multilateral forums to better understand the aviation security regimes currently in place in other countries in order to promote best practices while also enhancing current security systems, where necessary, in order to ensure commensurate levels of security from system to system. For example, TSA strives to harmonize security standards among those nations that are members of ICAO. Improved partnerships should increase security on high risk overseas flights through such initiatives as new international FAMS agreements and accelerated deployment of Advanced Imaging Technology. The U.S. aviation security partners anticipate that continued cooperation of our international partners will promote uniformity among nations.

3.1.4 Goal 4: Improve Situational Awareness, Understanding, and Collaboration Across the Aviation Transportation System

Objectives

- Enhance timely information-sharing among transportation sector partners.
- Advance resiliency concepts and risk management best practices within the aviation mode.
- Increase understanding of intermodal and cross-sector interdependencies and promote collaboration among modal partners.
- Develop and enhance preparedness and resiliency activities through plans, training, and exercises in collaboration with modal partners.

Improving situational awareness, understanding, and collaboration across the Aviation Transportation System is a critical, yet highly complex aspect of the missions of aviation modal partners. Due to the complexity and vastness of the aviation system, the mode's planning and implementation efforts are incremental and iterative in nature. Therefore, the mode intends to continue implementing its plan to accomplish this goal through its daily operations, as well as using focused programs and activities across three dimensions: intermodal and cross-sector collaboration, information sharing, and education and best practices. These foundational pillars comprise, at a high level, the mode's strategy in continuing this implementation process.

Collaboration and Information Sharing

As described in section 2.3, the ATS is comprised of Federal and State government agencies; Federal, State, and local law enforcement agencies; international partners; and industry stakeholders, such as airline and airport operators, vendors, and cargo movers. Collaboration among modal partners occurs strategically through coordination of policy, operationally through exchange of intelligence, and tactically through sharing of time-sensitive information. In this manner collaboration forges mutually beneficial relationships and helps to achieve shared outcomes.

The ATS is served by a significant web of information-sharing networks spanning a range of operational areas including air traffic control, threat intelligence, incident reporting, traveler alerts, and critical infrastructure conditions. As part of the implementation plan, efforts will continue to be targeted at improving overall network survivability through enhanced shared situational awareness and coordinated decisionmaking on real-time security incidents involving the NAS or otherwise affecting U.S. interests. Activities are continuously implemented to meet statutory requirements regarding information sharing and to support several strategies, including the National Information Sharing Strategy, the Intelligence Community Information Sharing Strategy, the DHS Information Sharing Strategy, and the Transportation Security Information Sharing Plan.

Federal agencies responsible for aviation safety and security have made, and will continue to make, significant investment in formal information-sharing venues serving protection, prevention, and emergency response needs through several full-time operations centers, including the TSOC, FAA's Washington Operations Center, CBP's Air-Marine Operations Center, the NICC, and the National Capital Region Coordination Center. These centers monitor aviation-related incidents, assess and disseminate timely information and intelligence to relevant stakeholders, and provide operational direction to Federal field offices. Real-time operational information on emerging incidents is shared among Federal aviation personnel, law enforcement, and airline operations with a need-to-know through multiple channels that include the Domestic Event Network (DEN). Information

is further disseminated through various agency and interagency facilities, such as State fusion centers and TSA airport coordination centers. Additionally, information for private industry stakeholders, such as Security Directives and Emergency Amendments will continue to be distributed through online WebBoards. However, efforts are being made to incorporate aviation modal industry partners into the developing HSIN-based Transportation ISAC as a mechanism for rapid distribution of unclassified threat information.

Currently, aviation security partners use the Automatic Detection and Processing Terminal (ADAPT) system to validate the identity of aircraft operating in or near the NAS and to serve as a critical advance warning system for air traffic controllers and security personnel. ADAPT allows users to validate the identity, threat posture, and movement of aircraft operating worldwide and displays the results in a user-friendly live radar picture. This system is currently operational and efforts continue to fully integrate ADAPT with additional government and commercial databases; however progress should continue towards a future state of enhanced collection of intelligence, including human and signals intelligence, the integration of all-source information, and the incorporation of computer-assisted anomaly detection to assist human analyses.

To combine the capabilities of both Aviation Domain Awareness, as envisioned by NextGen, and Maritime Domain Awareness, the aviation partners will work with the Office of the Director of National Intelligence who has initiated the Global Maritime and Air Intelligence Integration project to improve intelligence sharing within those domains. This initiative involves the development of an enterprise capability to support the collection, analysis, and dissemination of intelligence among United States and foreign government agencies responsible for law enforcement and aviation system security and regulation. Engaging within and across sectors ensures that the best practices and expertise are used to confront emerging risks. Recognizing this, aviation modal partners participate in information-sharing partnerships to counter cybersecurity threats.

Education and Best Practices

The aviation mode implements the awareness and collaboration goal through other Federal and corporate initiatives including the development of education programs and the dissemination of collaboratively generated best practices and standards. Internationally, TSA's Aviation Security Sustainable International Standards Team (ASSIST) program addresses the needs of partner nations to build sustainable aviation security practices through capacity development assistance. An important part of this effort is the aviation security training initiative which is designed to meet education needs of foreign aviation entities as identified by DHS, DOS, DOT, and foreign governments through Transportation Security Administration Representatives (TSARs). In order to bring about a sustainable increase in aviation security, TSA sends assistance teams to countries to help them meet ICAO standards. TSA also uses ASSIST teams to help foreign governments and aviation authorities build the capacity to apply international standards within their jurisdictions. These multi-faceted teams include members with varying types of expertise who identify areas of potential growth and development. TSA and the local authorities work in concert to reach mutually beneficial goals by sharing best practices, expanding educational opportunities, and building institutional capacity to achieve ICAO standards and U.S. requirements for carriers flying to the United States.

U. S. Government representatives function as liaison officers in a number of domestic and international posts. The liaison officers provide a stable presence in host countries and increase the awareness of aviation policies among foreign authorities, air carriers, shippers, and other international partners. International Industry Representatives (IIRs) liaise with foreign airlines and all-cargo air carriers, while TSARs and assessment teams in more than 20 countries inspect commercial airlines and air cargo services operating internationally, conduct foreign aircraft repair station outreach, and facilitate international intermodal and cross-sector understanding. These activities help to ensure security procedures are similarly developed and implemented across the globe, and best practices and strategies are appropriately applied.

Domestically, Federal Security Directors, aviation TSIs, and PSIs engage daily with airport authorities, airline operators, and associated vendors to identify protection and resiliency activities that work and those that do not. These collaborative evaluations helped to make local refinements to national initiatives such as checkpoint "Evolution." Frontline employees and airport

partners provided feedback on potential areas of improvement, best practices, and lessons learned. Greater emphasis on training has resulted in better networking among aviation partners, greater vigilance and insightful critical-thinking, and a more positive working environment. Implementing activities that promote industry awareness of security best practices and lessons learned support the TSA strategic focus on people, processes, technology, and partnerships.

3.2 Security Guidelines, Requirements, and Compliance and Assessment Processes

In addition to specific programs or projects to reduce risks, various aviation modal partners establish security-related guidance. In some cases, guidelines are developed by the government and international bodies, industry associations, or standards institutions. This type of guidance is typically voluntary. In other cases, guidance takes the form of a government requirement, such as regulations or security directives. Assessment and compliance processes have been developed to measure the degree to which the guidelines and requirements have been implemented and their impact on protection and resiliency goals.

3.2.1 Security Guidelines

Security guidelines are any formal protection and resiliency guidance recommended for implementation on a voluntary basis by airport owners and operators to enhance the protection of passengers, cargo, employees, and aviation infrastructure.

Recommended Security Guidelines for Airport Planning, Design, and Construction. On June 15, 2006, TSA issued revised “Recommended Security Guidelines for Airport Planning, Design and Construction” providing security guidance on airport layout, security screening, emergency response, access control and communications, and other topics. The Aviation Security Design Guidelines Working Group that created the guidelines was established under the ASAC and included representatives from ten government agencies and over 100 private sector experts. The guidelines assist professionals in the engineering, architecture, design, and construction fields to meet minimum standards for secure airport design and construction. This document is currently under review and will be updated as appropriate.

General Aviation Airport Security Guidelines/Information Publication. In May 2004, DHS and TSA, in cooperation with the general aviation industry, developed the General Aviation Airport Security Guidelines. The guidelines incorporate security best practices to assist individuals with oversight responsibility of general aviation airports and facilities regardless of size and type of operation.

Airport Watch/General Aviation Secure Hotline. The main security focus for recreational flying has centered on enhancing security at general aviation airports where the majority of operations occur. TSA developed and implemented the Airport Watch program to increase security vigilance with the flying public and direct industry to contact the General Aviation Secure Hotline (operated by TSOC) to report suspicious activities. This program provides a mechanism for any general aviation pilot or airport employee to report suspicious activities to Federal aviation modal partners through one focal point. TSA continues to operate the General Aviation Secure Hotline and promotes the use of the hotline through the See Something, Say Something campaign.

3.2.2 Security Requirements

Security requirements include regulations, security directives, emergency amendments, and standard or model security programs. These requirements may be enforced through civil penalty actions or restrictions on operations.

Security Regulations/Programs. Title 49 CFR establishes requirements for various classes of domestic and foreign air carriers, airports, flight schools, and private charter and commercial operators. Parties subject to these regulations are generally required to develop security programs for approval by TSA. Once approved, the programs become required standards for the regulated party.

Security requirements for certain aircraft operators are provided under 49 CFR Part 1544. Part 1544 outlines six distinct programs:

- Full program;
- Private charter standard security program;
- “Twelve-five” standard security program;
- Partial program;
- All-cargo standard security program; and
- Limited programs.

The required procedures include, but are not limited to, vetting passengers, inspecting aircraft, restricting access to certain areas of infrastructure and conveyances, screening people and cargo, and training flight personnel. Similarly, 49 CFR Part 1546 describes required security measures for foreign air carriers and outlines their need to adopt a Model Security Program.

Under 49 CFR Part 1542, baseline security requirements are provided for defined types of commercial airports. Under the regulation, airport operators must adopt and comply with an Airport Security Program (ASP). Once the airport operator develops an ASP, the FSD reviews and approves it, ensuring that all necessary security considerations are included and sufficiently addressed. When approved, compliance with the ASP is evaluated and enforced by TSA. A designated Airport Security Coordinator has custodial responsibility for the ASP and must inform TSA of any proposed changes.

Special rules for aviation operations in the District of Columbia are established under 49 Part CFR 1562. The Ronald Reagan Washington National Airport (DCA) Access Standard Security Programs (DASSP) permits the use of DCA by certain general aviation aircraft that apply for and comply with the regulation and program. The program requires crew and passenger vetting, baggage screening, increased security officer presence, and aircraft inspections. Additionally, the rule requires fixed-base operators to comply with the fixed-base operator standard security program.

In addition to standard security programs, other requirements, such as Airport Operating Certificates (AOCs), serve to ensure safety in air transportation. FAA issues AOCs to airports under 14 CFR Part 139 if scheduled passenger-carrying operations are conducted in aircraft designed for more than nine passenger seats. Airports must also hold an AOC if unscheduled passenger-carrying operations are conducted in aircraft designed for at least 31 passengers.

Non-certified airports, by contrast, are those airports with scheduled passenger-carrying operations of an air carrier operating aircraft designed for 30 passengers or less that include: 1) airports serving scheduled air carrier operations only by reason of being designated as an alternate airport; and 2) airports operated by the United States. FAA’s regulatory authority helps establish minimum safety standards for operations in airports that are critical to the NAS.

In response to the 9/11 Act, TSA developed and is implementing a standardized threat and vulnerability assessment for general aviation airports. For the initial roll-out of the program, TSA is working with industry to distribute the assessment to 3,000 general aviation airports meeting specific criteria. The assessment allows planners to assess the current vulnerabilities of the general aviation community and may lead to grants or other means of funding to improve security.

Security Directives and Emergency Amendments. Because of the ever-changing risks to commercial aviation, domestic aircraft operators, indirect air carriers, and foreign carriers must proactively develop and implement new procedures to mitigate threats to address security vulnerabilities. Security Directives (SDs) and Emergency Amendments (EAs) are security regulations issued on an emergency basis without a requirement for prior public notice. Based on specific intelligence information or other emergent circumstances, the government issues SDs/EAs to make rapid security adjustments. SDs/EAs require aircraft operators, domestic airport operators, and foreign air carriers to implement new security procedures, often on short notice. SDs/EAs address actions to reduce vulnerabilities, to provide security measures for travel to specified airports, and to adjust

procedures in response to changes in the Homeland Security Alert System. EAs address mandatory amendments to Standard Security Programs.

Maryland Three Rule (MD-3). This program authorizes the operation of three Maryland general aviation airports within the DCA flight restricted zone (FRZ). Airports must comply with the MD-3 security program, and pilots must be vetted by TSA and FAA and be issued a personal identification number to be permitted to file a flight plan into the FRZ.

3.2.3 Compliance and Assessment Processes

Compliance and assessment processes are used to oversee the implementation and adequacy of security measures and offer an overarching view of the security and safety posture of the ATS—its specialized and technical aspects and the patterns of compliance of aviation owners and operators. These processes can take the form of regulatory inspections, voluntary inspections, assessments of risk or its components, surveys, data calls, or other methods. Compliance and assessment results yield similar information about countermeasures or risk reduction initiatives that enable the modal managers to determine the effectiveness of ongoing initiatives or to identify gaps in protection and resiliency targets. Compliance inspections or visits generally apply to voluntary standards, regulations, or standard security programs. Assessments within the ATS refer to initial visits at the start of an inspection cycle, security threat assessments (background checks) of individuals, and evaluations of risk or risk components within critical infrastructure.

Compliance processes determine the degree to which voluntary or required guidelines are applied within a particular asset, system, or network. In the aviation mode, TSA manages several different compliance inspection regimes: air cargo, airports, airlines, general aviation, and “twelve-five” aircraft. TSA is responsible for enforcing aviation security regulations and programs and employs hundreds of TSIs at airports across the United States to conduct compliance inspections of air carriers and airports and to work with regulated entities to correct identified security deficiencies. Each aircraft operator is assigned a PSI to ensure overall security compliance at the corporate level.

TSA also deploys Transportation Security Specialists to specified foreign locations as necessary and directs them to conduct assessment under the Foreign Airport Assessment Program (FAAP) for compliance with ICAO standards and TSA requirements. Generally, TSA works with foreign governments and airports to improve operational implementation of ICAO standards and TSA requirements, including offering capacity development assistance. However, if the Secretary of Homeland Security finds, based on TSA’s assessment, that an airport has failed to implement appropriate security measures, the Secretary notifies foreign government authorities of that decision and recommends steps to achieve compliance. If the airport fails to comply within 90 days of such notice, DHS must publish a notice in the Federal Register that the airport is non-compliant, post its identity prominently at major U.S. airports, and notify the news media. In addition, U.S. aircraft operators and foreign air carriers providing transportation to the violating airport from the United States must provide written notice to ticketed passengers for flights to that airport of the airport’s non-compliant status. The Secretary may also “withhold, revoke, or prescribe conditions on the operating authority” of an airline that flies to that airport and the President may prohibit an airline from flying to or from said airport and a point in the United States.

Through IIRs, TSA is responsible for liaising with foreign air carriers and all-cargo aircraft carriers under the Foreign Air Carrier Security Program. Some 150 foreign air carriers and 30 cargo carriers have security programs with operations into the United States. Under the FAAP and Air Carrier Inspection Program, TSA assesses more than 300 Category A and B international airports, inspects more than 454 U.S. carrier stations overseas, and inspects more than 294 foreign air carrier stations with operations to the United States. Furthermore, TSA issued a Notice of Proposed Rulemaking on aircraft repair station security. The regulations authorizing this program will require that all FAA-certified Part 145 repair stations, domestic and foreign, comply with security regulations. Additionally, all foreign repair stations will be required to undergo a security review and audit. TSA manages the overall Aircraft Repair Station Program and has developed and implemented the Foreign Repair Station Program to ensure the security of maintenance and repair work conducted on U.S. aircraft operator and components

at domestic and foreign repair stations, as required in 49 USC 44924. There are 4,100 domestic and 700 foreign FAA-certified aircraft repair stations.

The FAA Facility Security Management Program (FSMP) establishes security requirements for all FAA facilities and standard procedures for facility security management, control, and safeguarding of personnel facilities. FAA security specialists conduct risk-based assessments and inspections to determine compliance with facility security, communications, security, classified information, national directives, and DOT policies that influence FAA security practices. The FSMP addresses security risk mitigation of the National Airspace System (NAS) and support elements to reduce, deter, and eliminate threats against FAA assets.

3.3 Decisionmaking Factors

The SSP provides general guidance for the Transportation Systems Sector regarding the risk management framework for protecting critical infrastructure and addressing resiliency objectives. Aviation modal partners apply this approach in reaching decisions about the criticality of aviation infrastructure, the risk associated with specific infrastructure, and its physical, human, and cyber components. Security decisions for the ATS are heavily influenced by information regarding threats. Threat information from historic and current intelligence analyses provides an understanding of the range of capabilities and intents of terrorists. Threats guide the development of consequence estimates and vulnerability assessments. Threat analysis is a key aspect of the risk management process in aviation. There is a significant possibility that adversaries could attack aviation infrastructure in ways that are not reflected in intelligence assessments. Consequently, one of the decision factors for risk mitigation is the presence of unknown threat.

This Aviation Modal Plan prioritizes programs and activities using a threat-based, risk management approach in order to appropriately allocate resources to the higher priority initiatives. Due to the diversity of infrastructure in the ATS and the volume of passengers and cargo, decisionmakers apply a comprehensive approach to consider all relevant factors including: costs; legal, moral, and ethical issues; physical and ergonomic constraints; mission effectiveness; and other pertinent factors.

The allocation of funding for grant programs also follows a systematic and thorough process. Funding distribution is based on priorities and objectives that are determined through risk assessments. Ultimately, key elements of the decisionmaking process influence program implementation throughout the ATS.

3.3.1 Program Implementation

Budgetary factors and implementation time are constraints that the ATS must take into account when prioritizing security needs and when developing specific programs. Resource limitations inherently compel Federal aviation modal partners to carefully analyze modal priorities and evaluate progress. Budgets, however, may evolve based on external conditions, new technologies, and management challenges that can prolong program development and implementation. These factors must be continually monitored and considered in the programmatic and policy planning and implementation processes.

The maintenance of security and protection programs—and their continued contribution to the sector's resiliency strategy—is a shared responsibility among aviation partners. The Federal partners are responsible for coordinating the planning, programming, budgeting steps, and the maintenance of federally-operated programs. Once programs are implemented, aviation security-related agencies are also responsible for providing standardized feedback and conducting annual surveys on the effectiveness and efficiency of their programs. This feedback is used to guide program sustainment or adjustment and to collect best practices and lessons learned in developing new programs. This process is integral in the full-cycle assessment of programmatic effectiveness and for the development of new programs and initiatives.

The success of any ATS security and protection program is based, in large part, on the input and cooperation of relevant modal partners. Coordination and communication with aviation modal partners is vital to ensure that any changes or termination of

Federal programs that will impact other programs are properly explained and efficiently carried out. Projects are monitored following implementation, and on an ongoing basis, to ensure that feedback is timely and effectively addressed.

Proper program design includes measures of effectiveness for each countermeasure. These metrics are then used to monitor the degree to which countermeasures are achieving their objectives. Output measures will assist in analyzing a program's ability to meet its milestones, while outcome measures will gauge a program's contribution to the aviation mode's risk mitigation objectives.

3.3.2 Grant Programs

DHS has several security grant programs and TSA provides technical assistance in evaluating grant proposals. TSA also provides technical recommendations for the FAA Airport Improvement Program (AIP) grants.

The AIP gives grants to public agencies and private entities for planning and developing public-use airports. A public-use airport is an airport open to the public that is publicly or privately owned, but designated by FAA as a "reliever," or privately owned but having scheduled service and at least 2,500 annual enplanements. An airport must be part of the National Plan of Integrated Airport Systems to qualify for a grant.

Grant funds may be used on projects related to improving or enhancing airport safety, capacity, security, and noise/environmental concerns. Grantees (referred to as sponsors) can use AIP funds on most airfield capital improvements and for some terminals, hangars, and non-aviation development projects.

Risk assessment for AIP funding occurs on both the national and local levels. The AIP process does not include an internal risk assessment study; rather external studies are referenced to determine priorities and objectives on the national level, as well as to define eligible projects for individual facilities.

Safety and security projects proposed for grant funding should conform to Federal regulations for airport certification procedures or design standards. These two project categories include obstruction lighting and removal, fire and rescue equipment, fencing, and access control systems. FAA gives safety and security development the highest priority to ensure rapid implementation and to achieve the highest possible level of safety and security. AIP funds are drawn from the Airport and Airway Trust Fund, which is supported by user fees, fuel taxes, and other similar revenue sources.

Immediately following the attacks on September 11, 2001, significant AIP grant funding was directed to security projects in FY 2002 and FY 2003. Changes to legislation regarding the funding of airport security projects resulted in AIP funding for security returning to pre-September 11, 2001 spending levels. This enabled FAA and airports to begin to address the backlog of reconstruction, rehabilitation, and standards projects that had built up over the two prior years as airport sponsors deferred work in order to accommodate security projects in FY 2002 and FY 2003. AIP grant funding for security projects currently totals approximately two percent of the program.

The Aviation Security Capital Fund provides \$250M per year for aviation security projects on a cost-shared basis through 2028 and is supplemented with further direct appropriations. The Fund has become the dominant grant mechanism for achieving aviation security programming in recent years, especially in funding the procurement and installation of in-line checked baggage explosive detection systems at airports.

3.3.3 Aviation Modal Plan Review Process

In conformance with the NIPP, the Aviation Modal Plan follows the same triennial revision cycle and annual review process as the SSP Base Plan. The Aviation Modal Plan relies on the participation of aviation modal partners. The AGCC, ASCC, and ASAC serve as a means for collaboration and coordination among aviation modal partners

For the preparation of the 2010 Aviation Modal Plan, the AGCC and the ASCC established a Joint Aviation Plan Working Group (JAPWG), under the auspices of the CIPAC, to consider revisions to the 2007 Aviation Modal Implementation Plan. The working group included representatives of the AGCC and ASCC member agencies and cyber and metrics specialists. The JAPWG was the primary collaborative body to review and revise the modal plan and will also assist in the annual processes to evaluate implementation of and revisions to the plan.

3.4 Performance Measurement

To evaluate the collective impact of the Transportation Systems Sector's efforts to mitigate risks and to increase the resilience of the transportation system through information-sharing mechanisms, measures of programmatic and policy effectiveness must be developed and monitored. These metrics supply information either to affirm that SSP goals and objectives are being met or to suggest corrective actions. This section provides an overview of the Transportation Systems Sector's strategy for measuring the effectiveness of risk reduction efforts.

3.4.1 Risk Mitigation Activities

The Transportation System Sector's RMAs are programs, tools, initiatives, projects, major tasks, or other undertakings that directly or indirectly lead to a reduction in risk. These activities meet or substantially contribute to the ATS's CIKR protection and resilience objectives outlined in section 3.1. For planning purposes, RMAs provide a mechanism to organize the key risk reduction areas and focus mitigation efforts on high priority risks within the mode. To facilitate intermodal and cross-sector relevance, RMAs have been segmented into the categories outlined in table A3-1.

Table A3-1: Key Aviation Modal Risk Mitigation Activities

Key Aviation Modal RMAs
• Security vetting of workers, travelers, and shippers
• Securing of critical physical infrastructure
• Implementation of risk mitigating operational practices
• Implementation of unpredictable operational deterrence
• Screening of workers, travelers, and cargo
• Security awareness and response training
• Preparedness and response exercises
• Awareness and preparedness
• Leveraging of technologies
• Transportation industry security planning
• Security programs and vulnerability assessments
• Securing of critical cyber infrastructure

3.4.2 Metrics

The aviation mode consistently measures performance and effectiveness in implementing risk management procedures and activities. In addition, it routinely assesses the performance of industry partners and their security procedures. This data is interpreted and used to inform programmatic and policy decisions made by Federal agencies.

In the ATS, metrics are used to track the progress of programs and initiatives, gauge whether they fulfill their performance objectives, and report output data. This process is fundamental to risk management initiatives, as it allows for collecting feedback on program performance and risk reduction. Outcome metrics are particularly useful in measuring a program or initiative's contribution to the mode's risk mitigation objectives. By aligning RMAs with standardized intermodal and cross-sector categories, aviation modal partners are able to evaluate comparable metrics of success. Specifically, TSA compiles measurement data on the following RMAs within the ATS's scope of security operations:

- **VIPR Team Events** – TSA measures the number of events that each VIPR team engages in and compares it to an established goal. This metric ensures that VIPR teams are being utilized sufficiently and appropriately across the Transportation Systems Sector.
- **TSA-Certified Canine Team Screening Hours** – Canine teams offer an unpredictable and flexible approach to risk mitigation, and TSA measures the number of hours that each team operates in relation to established goals.
- **Percentage of Cargo Screened on Passenger Aircraft** – In an effort to track progress on the CCSP mandate to screen 100 percent of air cargo on passenger aircraft within the United States, TSA continually monitors the percentage of cargo that undergoes screening procedures.
- **Unpredictable Drill Hours** – TSA frequently performs drills that test the operational effectiveness of security procedures at aviation modal facilities. The number of hours performing this task in relation to predetermined milestones is also measured. Particular efforts are made to ensure that unpredictable operations maintain widespread geographical and functional coverage.

These outcome metrics, among others, are compiled to aid in the direction and modification of programs and policies within aviation security and protection. By using objective measures of programmatic performance, the aviation community is able to collaboratively assess the progress of public and private efforts. Continued progress in measureable risk reduction requires the maintenance of the risk reductions already achieved. This necessitates the consistent and frequent monitoring of programmatic successes, targets, and goals. Targets and goals must be regularly evaluated and readjusted to reflect changing security conditions, postures, and progress. Aligning metrics with designated RMA categories facilitates modal, intermodal, and cross-sector efforts to achieve overall risk reduction.



4. Way Forward

The Federal Government has established a scalable, flexible ATS that is responsive to a range of current and future threats to the United States. Significant improvements to the aviation mode have been achieved by the layered security strategy, greatly reducing the likelihood of a successful attack. These enhancements and countermeasures represent important steps forward; however, no individual component is completely fail-safe. Moreover, terrorists are continuing to devise methods for defeating security efforts, as evidenced by the threats to U.S.-bound flights identified by officials in the United Kingdom. The aviation mode is developing long-term and near-term objectives to address security and safety concerns of the next generation ATS.

4.1 Long-Term Aviation Objectives

Several forward-thinking government initiatives are reconsidering present approaches to aviation security and protection. In particular, aviation modal partners are working collaboratively to plan the NGATS and the “airport of the future,” by incorporating new and emerging technologies to reduce the operational impacts of protection and resiliency measures. “Airport of the future” is defined as the integration of the array of NextGen technologies and/or operational processes and procedures planned to significantly enhance security measures in the future. These enhancements include new technologies, the integration of these technologies among security partners, and the design and continual development of technological enhancements. The objective is to more effectively apply risk management techniques, thus enabling U.S. air commerce to meet expected growth safely and securely.

FAA's JPDO was established by the Vision 100—Century of Aviation Reauthorization Act of 2003 through Public Law 108-176. Its mission is to address the requirements for the NGATS by:

- Creating and carrying out the Integrated Work Plan;
- Coordinating aviation research programs;
- Coordinating goals, priorities, and research activities within the Federal Government;
- Coordinating the development and utilization of new technologies; and
- Facilitating technology transfer among Federal departments and agencies and the private and public sectors.

The vision is to accommodate an anticipated increase in demand, while ensuring a superior level of safety, efficiency, and security that has been the hallmark of the American aviation system. With a focus on safety, security, the environment, and international cooperation, the JPDO's NextGen Aviation Security Working Group will work cooperatively with development teams to leverage resources to design and implement a security infrastructure that will ensure a robust and secure ATS. NextGen implementation objectives include:

- Enhance NextGen's Integrated Risk Management framework, which includes prognostic tools, models, and simulations at the strategic, operational, and tactical levels, including nominal and off-nominal situations, to support all decisionmakers with cost-effective best practices for the design, acquisition, deployment, and operation of aviation security system assets and infrastructures.
- Continue to expand NextGen implementation capabilities to encompass a robust set of strategic, tactical, and operational capabilities and services focused on detection, prevention, protection, response and mitigation, and recovery initiatives that are undertaken by a variety of aviation modal partners.
- Develop NextGen Airport network-enabled operations that seamlessly link sensors and data sources from access and screening checkpoints for passengers, visitors, employees and vehicles, perimeters, and critical facility infrastructure.
- Increase NextGen stakeholder involvement to foster industry, Federal, and local partnerships with clearly defined roles and responsibilities for prevention, protection, mitigation, response, and recovery operations at strategic, operational, and tactical levels.

4.2 Near-Term Aviation Objectives

Given the strategic goals identified previously, the mode has identified the following actions to advance aviation protection and resiliency objectives over the next three years.

Goal 1: Prevent and Deter Acts of Terrorism Using or Against the Air Transportation System

- Enhance effectiveness of international FAMS agreements.
- Launch and implement an enhanced Insider Threat Mitigation Program.
- Advance flexible, unpredictable screening methods (e.g., VIPR, Playbook, Risk Emphasized Flight Screening, and Aviation Screening Assessment Program).
- Collaborate with other agencies and aviation modal partners to mitigate insider, cyber, and chemical, biological, radiological, nuclear, and explosive (CBRNE) threats.
- Develop deployable sensor systems to detect and otherwise mitigate threats from hijacking/unauthorized diversion, explosive destruction, external attack, onboard CBRNE, or other attack of crew, passengers, or aircraft systems.
- For air cargo in the next several years, TSA's primary efforts will center on the CCSP. Successful implementation of the program by the government and widespread acceptance of the program by industry will have profound positive effects on the air cargo industry.
- Develop Secure Airspace access and flight procedures based on a verification process that dynamically adjusts for aircraft performance and security considerations (NextGen Integrated Risk Management).
- Continue to evolve ADAPT and other shared situational awareness platforms to enable dynamically adjustable airspace boundaries and access criteria of Security Restricted Airspace, Special Use Airspace, and Temporary Flight Restrictions.
- Further develop the remote terminal security screening concept to continue to move the security perimeter further away from the airport.
- Develop similar security measures and practices for the emerging unmanned aircraft systems and expected commercial spacecraft or sub-orbital systems.

Goal 2: Enhance the All-Hazard Preparedness and Resilience of the Aviation Transportation System to Safeguard U.S. National Interests

- Expand the ATS's preparedness across the prevention, protection, response, and recovery spectrum.
- Encourage development of awareness and preparedness initiatives to enhance continuity of ATS operations.

Goal 3: Improve the Effective Use of Resources for Transportation Security

- Identify technological opportunities to improve and expedite passenger and cargo screening capacity and capabilities.
- Develop metrics for costing security initiatives and risk reduction measures.
- Create an acquisition strategy that drives continued technical innovation while procuring needed state-of-the-art equipment.
- Establish a process for long-range strategic planning to ensure research and development activity is coordinated and aligned with NextGen goals and objectives.
- Develop, with DHS, a Center of Excellence for canine capabilities.

Goal 4: Improve Situational Awareness, Understanding, and Collaboration Across the Aviation Transportation System

- Establish a seamless information sharing process across modal segments (airlines, airports, and national command centers).
- Develop a usable cross-modal consequence model for evaluating threat impacts on sector-wide and ATS CIKR.
- Enhance awareness and assessments of interdependencies between modes and across sectors domestically and internationally.
- Increase programs at State, local, tribal, and owner and operator levels to maintain awareness of employees and the traveling public regarding security threat identification and reporting.
- Enhance international cooperation through partnerships with foreign governments and through international security standards for container security and collection of biometric data for incoming international passengers.
- Deploy ASSIST to evaluate and build the aviation security capacity of foreign partners identified as having the need and the will to enhance aviation security.
- Build stronger international partnerships to raise overseas security levels for passengers, baggage, and cargo.
- Develop plans and procedures to ensure continuity of operations for cyber information and control systems that support the operations of the aviation industry.
- Enhance public-private engagement to improve the state of security of critical cyber assets, systems, and networks.

Aviation security remains a preeminent priority among Federal aviation partners, who continue to evaluate and update modal risk management approaches. This section has highlighted some of the forward-leaning initiatives to address identified threats and vulnerabilities. Given the ever-changing threat environment, Federal aviation modal partners must continually reexamine the programs and policies in place to maximize relevancy and effectiveness. With this in mind, a risk management approach must be flexible and informed, incorporating all relevant entities, resources, and partners. Federal aviation modal partners must strive to achieve improvements in the targeted areas above, while also frequently analyzing progress and strategy.



Appendix 1: Matrix of Aviation Programs and Activities

Programs and Activities	Responsible Agency
Transportation Security Lessons Learned Information Sharing (LLIS)	DHS/TSA
Homeland Security Advisory System (HSAS)	DHS
Continuity of Operations Program (COOP)	DHS/ALL
Visible Intermodal Prevention and Response (VIPR)	TSA
Customs-Trade Partnership Against Terrorism (C-TPAT)	CBP/TSA
NEDCTP Rapid Deployment Canine Team Force (NRDCTF)	TSA
National Infrastructure Coordination Center (NICC)	TSA
Transportation Security Operations Center (TSOC)	TSA
Transportation Worker Identification Credential (TWIC)	TSA
FAA Information Security Systems (ISS)	FAA
Facility Security Management Program	FAA
Visitor Vetting and Control	FAA
Mail and Delivery Screening	FAA
HSPD-12 Joint Program Office Initiatives	FAA
Personnel Security	FAA
Air Traffic Security Coordinator (ATSC)/Air Defense Liaisons (ADLs)	FAA/TSA
Aviation Worker Background Check Program (AWBCP)	TSA

Programs and Activities	Responsible Agency
Domestic Events Network (DEN)	FAA/TSA
Federal Air Marshal Service (FAMS) Mission Deployments	TSA
FAMS Force Multiplier (FAMSFM) Program	TSA
Federal Flight Deck Officer (FFDO) Program	TSA
National Capital Region Coordination Center (NCRCC)	TSA
Registered Traveler	TSA
Secure Flight Program	TSA
Temporary Flight Restrictions	FAA, TSA
Tactical Information Sharing System	TSA
Aircraft Operator Standard Security Program (AOSSP) and Security Directives (SDs)	TSA
Inspection, Investigative, and Enforcement Procedures	TSA
Airport Liaison Agent (ALA) Program	DOJ/FBI
Airport Security Consortia (Local Advisory Committee)	TSA
Improved Airport Perimeter Access Security (Aviation and Transportation Security Act [ATSA] Section 106)	TSA
Airport Emergency Plan (AEP)	FAA, TSA
Investigative and Enforcement Procedures Airport Inspection Program (Annual Work Plan)	TSA
Under 49 CFR, Part 1542 <ul style="list-style-type: none"> • Airport Security Program (ASP) • Homeland Security Advisory Threat Condition Enhancements (Aviation Security [AVSEC] Levels) • Airport Tenant Security Program (ATSP) • Aircraft Operator or Foreign Air Carrier Exclusive Area Agreements 	TSA
Recommended Security Guidelines for Airport Planning, Design, and Construction Document, dated June 15, 2006	TSA
Backscatter	TSA
Document Scanners	TSA
Explosives Trace Detection (ETD) (Checkpoint Operations)	TSA
Handheld Metal Detectors (HHMDs)	TSA

Programs and Activities	Responsible Agency
Screening of Passengers by Observation Techniques (SPOT) Program	TSA
Checkpoint Screening (Checkpoint Operations)	TSA
Threat Image Projection (TIP) Ready X-Ray (TRX)	TSA
Trace Portal	TSA
Walk-Through Metal Detectors (WTMDs)	TSA
Approved Alternative Screening Procedures (Checked Baggage Operations)	TSA
Explosive Detection Systems (EDS) (Checked Baggage Operations)	TSA
Explosives Trace Detection Equipment (Checked Baggage Operations)	TSA
Secondary Screening (Checked Baggage Operations)	TSA
Air Cargo Watch Program	TSA
Certified Cargo Standard Security Program (CCSP)	TSA
Full Air-Cargo Aircraft Operator Standard Security Program (FACAOSSP)	TSA
Indirect Air Carrier Standard Security Program (IACSSP)	TSA
Air Cargo Freight Assessment System (FAS)	TSA
Air Cargo Regulatory Compliance Inspections, Investigations, and Enforcement Procedures	TSA
Known Shipper Management System (KSMS)	TSA
Indirect Air Carrier Management System (IACMS)	TSA
Air Cargo Vulnerability Assessments	TSA
Air Cargo Screening Technology Pilot	TSA
Narrow-Body Amendment	TSA
GA-SECURE Hotline	TSA
Armed Security Officer (ASO) Program	TSA
Alien Flight Student Program	TSA
Information Publication: "Security Guidelines for General Aviation Airports"	TSA
Maryland Three (MD-3) Program	TSA

Programs and Activities	Responsible Agency
Ronald Reagan Washington National Airport Access Standard Security Programs (DASSP)	TSA
Private Charter Standard Security Program	TSA
Transportation Security Administration Access Certificate: TSAAC Protocol	TSA
Twelve-Five Standard Security Program	TSA
Foreign Airport Assessment Program (FAAP) and air carrier (domestic aircraft operator and foreign air carrier) inspection activities to meet ICAO standards and TSA requirements (in accordance with 49 U.S.C. §§ 44905 and 44907)	TSA
Transportation Security Administration Representative liaison (bilateral and multilateral), crisis management, information sharing, and national aviation security activities in accordance with 49 U.S.C. 44934	TSA
Foreign Air Carrier Model Security Program (MSP) and Emergency Amendments (EAs) under 49 U.S.C. 44906 and 49 CFR part 1546; international measures contained in the Aircraft Operator Standard Security Program (AOSSP) and domestic aircraft operator Security Directives (SDs) under 49 CFR part 1544	TSA
International TSS and FAM missions and deployments	TSA
APIS implementation	CBP
International Industry Representative foreign air carrier liaison and overseas air carrier station visit activities	TSA
Multilateral organization liaison activities	TSA
Capacity development and technical aviation security training activities	TSA
Foreign (Aircraft) Repair Station (FRS) program	FAA/TSA
DOS air services agreements and Anti-Terrorism Assistance Program (ATAP)	DOS
Economic authority and operating licenses, including International Aviation Safety Assessment (IASA) oversight and airline safety liaison activities	DOT/FAA
Bomb Appraisal Officer (BAO)	TSA
Threat Containment Unit (TCU)	TSA
Counter Man-Portable Air Defense Systems (MANPADS) Vulnerability Assessment Program	FAA/TSA

Annex B: Maritime

The National Maritime Transportation Security Plan for input to the Transportation Systems Sector-Specific Plan.¹

¹ As required by the Maritime Transportation Security Act of 2002, the NMTSP was developed and signed in 2005 and promulgated in 2006. This Maritime Annex, as originally intended, is now the NMTSP and is considered to be a component of the TS SSP and not subservient to it. Appendixes not enclosed in this publication shall be issued separately and may vary in classification. The TS SSP base plan now fulfills National Strategy for Transportation Security 2005 and NIPP 2009 requirements.



Contents

Preface	169
1. Executive Summary	171
2. The Overview of the Mode	173
2.1 The Maritime Mode	175
2.2 Unique Characteristics of the Maritime Transportation Mode: Assets, Systems, and Networks.	176
2.3 Risk Considerations	181
2.4 Framework for Partnership and Information Sharing	183
3. The Implementation Plan	187
3.1 Vision, Goals, and Objectives	188
3.2 Strategic Risk in the MTS	189
3.3 Assessing Risk and Prioritizing Assets and Systems: Tactical/Operational Risk Planning.	190
3.4 Decisionmaking Factors	191
3.5 Programs, Initiatives, and Risk Mitigation Activities	192
3.6 Metrics/Measurement Process	196
4. Security Gaps	199
4.1 Security Guidelines	199
4.2 Security Requirements	200
4.3 Assessment and Compliance Process	201
4.4 Training and Exercises	201
4.5 Grant Programs	201
4.6 Challenges for MTS Operations	201
5. The Way Forward	203
Appendix A: Related Plans and Strategies	205

List of Figures

Figure B2-1: Maritime Security Levels	180
Figure B3-1: Relationship of Maritime Security Plans per HSPD-13 and HSPD-7	187
Figure B3-2: NIPP Risk Management Framework	190



Preface

The Maritime Modal Annex (2007) and the National Maritime Transportation Security Plan (NMTSP) (2005) together, were the input to the Transportation Systems Sector-Specific Plan (TS SSP) (2007) in support of the National Infrastructure Protection Plan (NIPP) (2006). Since that time, the NIPP (2009) has undergone revision and the TS SSP (2010) reflects a shift to a more holistic view, including all-hazards considerations across physical, cyber, and human risk elements. For the purposes of efficiency, the TS SSP now incorporates other national planning requirements, such as the National Strategy for Transportation Security and other modal security plans of national scope. This annex serves concurrently as the Maritime Modal Annex to the TS SSP and the NMTSP as required by 46 United States Code (U.S.C.) 70103. The prior version of the NMTSP is superseded.²

There are 18 critical infrastructure and key resources (CIKR) sectors, each with Sector-Specific Agency (SSA) designations. One of these sectors is Transportation Systems and the Transportation Security Administration is the designated SSA. The U.S. Coast Guard (USCG) is the SSA for the maritime mode, of the Transportation Systems Sector, as designated by the NIPP, and collaborates with the Transportation Security Administration.

Nothing in this plan alters or impedes the ability of the authorities of Federal departments and agencies to perform their responsibilities under law. This plan is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable by law or in equity, against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.

This plan contains five sections and five appendices:

Section 1: Executive Summary.

Section 2: The Overview of the Mode. Narrative descriptions of the Maritime Transportation System, from a national-level perspective, along with existing information-sharing mechanisms. Contains the features of assets, systems, and networks, including the associated physical, cyber, and human risk elements of critical infrastructure.

Section 3: The Implementation Plan. Describes the goals and strategic and operational risk, including renewed emphasis on the cyber risk element, for the maritime mode. Additionally identifies assets, systems, networks, and functions and details the models, methods, and tools and performance measures that inform decisionmaking.

Section 4: Security Gaps. Details the effective practices that are applied to identify and mitigate security gaps.

² Section VI, Plan to Re-establish Cargo Flow After a Transportation Security Incident, and appendix B, National Roles and Responsibilities, remain in effect.

Section 5: *The Way Forward*. Explains efforts to reduce risk and enhance resilience, including emphasis on furthering understanding and awareness, increasing cooperative efforts through maritime regimes, and enhancing prevention, protection, response, and recovery capabilities.

Appendixes:

A: Related Plans and Strategies

B: National Roles and Responsibilities³

C: Plan to Re-establish Cargo Flow After a Transportation Security Incident⁴

D: Maritime Security (MARSEC) Levels⁵

E: Maritime Enterprise Mapping: Directives and Guidance⁶

³ Contains Sensitive Security Information (SSI) and is not included herein.

⁴ Contains SSI and is not included herein.

⁵ Future appendix (For Official Use Only (FOUO)) and is not included herein.

⁶ Used as a work plan to guide Maritime Government Coordinating Council activities (FOUO) and is not included herein.

1. Executive Summary

Water covers more than two-thirds of the Earth's surface. These waters comprise an immense maritime domain, a continuous body of water that is the Earth's greatest defining geographic feature. Ships plying the maritime domain⁷ are the primary mode of transportation for world trade, carrying more than 80 percent⁸ of the world's trade by volume. U.S. maritime trade is integral to the global economy, representing 10.68 percent of global trade generated in 2008.⁹ From a system-of-systems perspective, the Maritime Transportation System (MTS)¹⁰ is a network of maritime operations interfacing with shoreside operations at intermodal connections and is part of global supply chains or domestic commercial operations. The various operations within the MTS network have components that include vessels; port facilities; waterways and waterway infrastructure; railroads; bridges; highways; tunnels; intermodal physical, cyber, and human connections; and users. Through the MTS, the maritime mode is the primary transportation mode providing connectivity between the United States and global economies; 99 percent of overseas trade by volume enters or leaves the United States by ship.¹¹ The MTS enables the United States to project a military presence across the globe, creates jobs that support local economies, and provides a source of recreation for all Americans. The Nation's economic and military security fundamentally relies upon the health and functionality of the MTS.¹²

The security of the MTS is paramount for protecting the Nation and its economy; however, it presents daunting and unique challenges for managers of the maritime mode. The security of the MTS is inextricably linked to the security of the maritime domain, which contains CIKR from many of the other critical infrastructure sectors and the Transportation Systems Sector modes. Ensuring the security of the MTS depends on understanding the diverse activities occurring in the maritime, land, air, and cyber domains through the transparency of all sector and transportation modal infrastructure and security activities.

The October 2005 National Maritime Transportation System Security Recommendations¹³ for the National Strategy for Maritime Security describe Maritime Transportation System Security as:

⁷ The National Strategy for Maritime Security (NSMS) defines the maritime domain "as all areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean, or other navigable waterway, including all maritime-related activities, infrastructure, people, cargo, and vessels and other conveyances. Note: The maritime domain for the United States includes the Great Lakes and all navigable inland waterways, such as the Mississippi River and the Intra-Coastal Waterway," p. 1, footnote 1.

⁸ United Nations Conference on Trade and Development, Geneva; Review of Maritime Transport 2008, Report by the Secretariat, p. xiii.

⁹ United Nations Conference on Trade and Development, Geneva; Review of Maritime Transport 2009, Report by the Secretariat, p. 83.

¹⁰ Also referred to as the Marine Transportation System; An Assessment of the U.S. Marine Transportation System, A Report to Congress (DOT, 1999). In the context of the Transportation Systems Sector, the USCG is the SSA for the maritime mode, which may also be referred to as the Maritime Transportation System mode.

¹¹ Committee on the Marine Transportation System, What Is the Marine Transportation System?, <http://www.cmts.gov/whatismts.htm>.

¹² Interagency Task Force on Coast Guard Roles and Missions, A Coast Guard for the Twenty-First Century: Report of the Interagency Task Force on U.S. Coast Guard Roles and Missions, December 1999.

¹³ NSPD-41/HSPD-13 established a Maritime Security Policy Coordinating Committee, which provided these recommendations.

A systems-oriented security regime built upon layers of protection and defense-in-depth that effectively mitigates critical system security risks, while preserving the functionality and efficiency of the MTS. Understanding that the most effective security risk management strategies involves cooperation and participation of both domestic and international stakeholders acting at strategic points in the system, the United States seeks to improve security through a cooperative and cohesive effort involving all stakeholders.

A list of related plans and strategies is appendix A.

Maritime transportation CIKR partners will achieve a safer, more secure, efficient, and resilient MTS through the cooperative pursuit of actions that mitigate the overall risk to the physical, cyber, and human CIKR assets and resources of the system and its interconnecting links with other modes of transportation and CIKR sectors:¹⁴

Information sharing is a key activity for preventing terrorist attacks and reducing America's vulnerability from all-hazard events across the physical, human, and cyber risk elements.¹⁵ Fully understanding threats, disrupting operations, and countering terrorist capabilities require the sharing of timely information. Information-sharing processes are at the core of the CIKR sector partnership model and both the public and private sectors look at ways to enhance effective information sharing.

Maritime Domain Awareness (MDA) allows for the effective understanding of anything associated with the global maritime domain that impacts the security, safety, economy, or environment of the United States and must be promoted. MDA is a foundational element of maritime security and CIKR protection. It enhances information sharing among Federal, State, local, and tribal authorities; the private sector; and international partners. This information is used by decisionmakers to determine response and risk management calculations to protect maritime CIKR and, in turn, the overall MTS. Awareness is key as an evolving incident or event unfolds. From a national to a local level, executive agents, CIKR partners, operational centers, and/or Unified Command decisionmakers must have situational awareness to implement effective incident response and recovery protocols.

Key to the protection of CIKR is the Maritime Security Risk Analysis Model (MSRAM). MSRAM is an effective tool used by decisionmakers at various levels to make informed decisions and to identify and manage risk to infrastructure in the maritime domain. A systems approach to risk identification and management improves the accuracy of a common operating picture and increases the potential for the efficient use of limited resources. MSRAM data is shared with the National Infrastructure Coordinating Center (NICC) and other transportation modes, as well as with other CIKR sectors.

Widespread international cyber attacks reflect the increasing importance of securing information systems in the MTS;¹⁶ the Nation must be protected against cyber risk elements and be made more resilient through the application of a flexible and adaptable cyber incident response capability. The exploitation of cyberspace could place critical systems, networks, and data at risk. Ongoing efforts, including engagement within the sector partnership model, are expected to continue in order to expand the knowledge and understanding of the cyber risk element and further mitigate risk to the MTS.

The measurement, or metrics, of the progress made toward achieving national-level goals and objectives, as described herein, is fundamental to ensuring the efficient alignment of resources to the highest priority of risk identified in the MTS. Risk Mitigation Activities (RMAs), from which programs and activities cascade, are categorized as (1) Risk Reduction Tools and Methods, (2) Maritime Security and Response Operations, (3) Maritime Domain Awareness, and (4) Effective Maritime Security Regimes. Information-sharing programs and activities cascade across all four categories. Both qualitative and quantitative metrics are reported in the Threat of Terrorism to U.S. Ports and Vessels, DHS Annual Report to Congress, and in the CIKR National Annual Report, as well as in other reporting venues.

¹⁴ Transportation Systems Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan, Maritime Annex, May 2007.

¹⁵ National Infrastructure Protection Plan, 2009.

¹⁶ Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland, February 2010.

2. The Overview of the Mode

The MTS is a complex system that is both geographically and physically diverse in character and operation. The unique qualities of the mode present extraordinarily complex challenges for those charged with the security of the MTS, including maritime CIKR assets and systems. From a system-of-systems perspective, the MTS is a network of maritime operations that interface with shoreside operations at intermodal connections and as part of global supply chains or domestic commercial operations. The various operations within the MTS network have components that include vessels; port facilities; waterways and waterway infrastructure; railroads; bridges; highways; tunnels; intermodal physical, cyber, and human connections; and users. The United States, like many other nations, works toward maintaining a balance between safe, secure ports and facilitating trade to promote economic growth.

... today, international trade has evolved to the point where almost no nation can be fully self-sufficient. Every country is involved, at one level or another, in the process of selling what it produces and acquiring what it lacks: none can be dependent only on its domestic resources. Global trade has fostered an interdependency and interconnectivity between peoples who would previously have considered themselves completely unconnected.¹⁷

The strategic objective of this plan is to enhance the domestic security of the United States—to prevent terrorist attacks, reduce America’s vulnerability to all hazards, minimize damage from events that do occur, enhance timely information sharing, and facilitate the recovery of maritime CIKR and the supply chain from transportation disruptions. A system of security functions, comprised of five elements, help to achieve these objectives:

1. *Awareness.* Identify and understand threats, assess vulnerabilities, determine potential impacts, and disseminate timely information to security partners and the American public.
2. *Prevention.* Detect, deter, and mitigate threats to the United States.
3. *Protection.* Safeguard the American people and their freedoms, critical infrastructure, property, and the U.S. economy from acts of terrorism, natural disasters, or other emergencies.
4. *Response.* Lead, manage, and coordinate the national response to all hazards.
5. *Recovery.* Facilitate short-term national, State, local, and private sector efforts to restore basic functions and services and MTS infrastructure after a transportation disruption during the response phase of incident management and help set the stage for long-term recovery.

Many factors influence decisionmakers when it comes to conducting RMAs across physical, cyber, and human elements. Among these factors are executive mandates, legislative mandates, leadership priorities, budget constraints, time requirements, and risk assessments. No single public or private sector entity possesses the responsibility, the resources required, or the

¹⁷ International Maritime Organization, Maritime Knowledge Centre, International Shipping and World Trade, Facts and Figures, October 2009, p. 7.

awareness needed for ensuring security in the MTS in an all-hazards environment. The security of the mode depends on the cooperative actions of multiple Federal, State, local, tribal, and private entities, in addition to international partners. The USCG is the SSA for the maritime mode and in a lead Federal agency (LFA) role, the USCG facilitates and coordinates Combating Maritime Terrorism (CMT) operations with other Federal, State, local, and tribal agencies to prevent, disrupt, protect, respond to, and recover from terrorism-related risks in the maritime domain.¹⁸ The FBI is also an LFA in combating terrorism and jointly works with the USCG in supporting uninterrupted MTS operations.¹⁹ A description of Federal agency duties and responsibilities under the Maritime Transportation Security Act of 2002 (MTSA, Public Law 107-295) can be found in appendix B.

MTS components share critical interfaces with each other through limited and selective overarching information systems. Improving the security of the MTS focuses on four primary elements: (1) Component Security, (2) Interface Security, (3) Information Security, and (4) Network Security. MTS component security ensures that individual physical components have measures in place to prevent exploitation, protect against terrorist attack, contain incidents that do occur, and recover from incident effects. MTS interface security provides for coordinated security measures between modes of transportation and at key intersections between MTS components and functions. MTS information security ensures that key data systems are not corrupted or exploited and are available to support maritime operations, while also providing the protected availability of proprietary information needed to support security planning and implementation. Network security is the big picture view that focuses on enhancing security through overarching systems that facilitate the performance of the MTS and provide effective coordination among stakeholders at the policy and senior management levels.

The maritime domain also contains CIKR from many of the other critical infrastructure sectors and Transportation Systems Sector modes. Providing for the security of the maritime mode depends on understanding all activities in the maritime domain through the transparency of all CIKR sectors and transportation modal infrastructure and security activities. The MTS and component CIKR function as intermodal gateways for cargo flow to and from other CIKR sectors. Significant economic and functional dependence within the transportation system is based on the timely and free flow of maritime commerce to and from U.S. destinations. Because of the complexity, these dependencies and interdependencies require maritime security planning to be coordinated and to consider the physical, cyber, and human environment. It is critical that public and private entities work together to ensure security grant funds are applied effectively and efficiently across the full spectrum of the Transportation Systems Sector.

The National Strategy for Maritime Security (NSMS) defines MDA as “the effective understanding of anything associated with the global maritime domain that could impact the security, safety, economy, or environment of the United States.” MDA has four activities: (1) collection, (2) fusion, (3) analysis, and (4) dissemination. Data and information on people, cargo, vessels, and infrastructure associated with the maritime domain are collected from all sources²⁰ via the concerted efforts of Federal, State, and local partners in conjunction with commercial stakeholders, foreign governments, and other international partners. The data sets are then fused and analyzed to provide situational awareness and reveal anomalies and patterns. The resultant intelligence and information are then available via a variety of communication channels. MDA is a foundational element for security and CIKR protection as it can:

- When properly shared, leverage a broad range of blue forces capabilities and authorities in a common purpose across Federal, State, local, and tribal governments as well as commercial and private entities
- Deter adverse behavior as players know that their actions are visible to authorities
- Enable authorities to sufficiently understand patterns of behavior and the domain so as to be able to intervene and prevent adverse events, or minimize consequences through rapid, coordinated, and effective response.

¹⁸ United States Coast Guard, Combating Maritime Terrorism Strategic and Performance Plan, June 2008, p. 23.

¹⁹ Annex II to NSPD-46/HSPD-15, U.S. Policy and Strategy in the War on Terror, designates the FBI as the LFA for the operational response to terrorist incidents in the United States, including the use of a weapon of mass destruction.

²⁰ All sources can be defined as classified sources, regulatory data, industry data, law enforcement, military, open sources, etc.

Consistent with its broad suite of legal authorities and jurisdiction, the USCG exercises SSA leadership for anti-terrorism prevention, protection, and facilitation of recovery for maritime CIKR and the domestic and international maritime supply chain. The strategic vision and requirements for the protection of the MTS, its CIKR, and the supply chain are translated into preparedness for practical application by engaging partners and stakeholders in the government and private sectors, and developing and exercising policies, plans, and procedures at the local, regional, and national levels. Maritime CIKR is addressed as part of the overall MTS, taking into consideration dependencies and the potential for transportation disruptions affecting CIKR throughout the system, including exploitation of commerce as a threat vector.

The Ports, Waterways, and Coastal Security (PWCS)²¹ mission leverages the SSA's presence in and near U.S. ports, as well as Captain of the Port (COTP) authorities; the special relationship the agency has with other government agencies, including at the local level; and the relationship with the maritime industry and other port-area stakeholders with maritime equities. Taken as a whole, this provides the basis for layered security in the maritime domain. The USCG CMT Strategic Plan involves a three-pronged strategic approach to accomplishing PWCS mission elements in cooperation with the programs and activities of maritime partners and stakeholders. These activities are focused primarily on the Nation's most economically and militarily strategic ports, although maritime security coverage extends to all ports and waterway areas. The level of each of these activities depends on which Maritime Security (MARSEC) level is set.

The core components of the CMT are MDA, Maritime Security Regimes, and Maritime Operations. Maritime Security Regimes refer to regulatory efforts, as well as domestic and international outreach and partnering efforts. Maritime Operations refer to actual operations, boardings, and escorts conducted by personnel on cutters, boats, and aircraft, and at shoreside. These components are listed as three separate actions; however, they overlap considerably, are pursued simultaneously, and reinforce USCG missions, including maritime law enforcement, enforcement of laws and treaties, and port and marine safety.

The largest aggregation of cargo within the Transportation Systems Sector occurs in ports—in vessels, cargo transfer and storage nodes, and intermodal connections. All are, to varying degrees, potential targets. The presence of cargo and conveyance, in close proximity to surrounding industrial areas and communities, magnify the potential consequences of even a single-facility or single-vessel Transportation Security Incident (TSI) to produce effects beyond the maritime domain. Vessels, containers, cargo, and commercial vehicles are also potential media for smuggling and infiltration of weapons and perpetrators, as well as potential conveyances of devices for direct attacks on port complexes. The Plan to Re-Establish Cargo Flow After a TSI is appendix C.

2.1 The Maritime Mode

As previously discussed, the MTS is a complex system that is both geographically and physically diverse in character and operation. The MTS consists of waterways, ports, and intermodal landside connections that allow the various modes of transportation to move people and goods to, from, and on the water. The MTS includes:²²

- 25,000 linear miles of navigable waters, including inland waterways
- 238 locks at 192 locations
- The Great Lakes
- The Saint Lawrence Seaway

²¹ PWCS is identified as a USCG-specific mission; security partners are encouraged to support this effort, which is often mutually reinforcing. PWCS mission elements are: (1) prevent and disrupt terrorist attacks, sabotage, espionage, or subversive acts in the maritime domain and the MTS; (2) protect the maritime domain and the MTS; (3) respond to and recover from attacks that do occur in the maritime domain and the MTS; and (4) deny the use and exploitation of the MTS by terrorists as a means for attacks on U.S. Territory, population centers, vessels, and maritime CIKR.

²² Additional information is available from the Committee on the Marine Transportation System, *What Is the Marine Transportation System?*, <http://www.cmts.gov/whatismts.htm>, updated May 2009. The MTS is also characterized by *An Assessment of the U.S. Marine Transportation System, A Report to Congress* (DOT, 1999).

- More than 3,700 marine terminals
- More than 1,400 intermodal connections

The maritime domain of the United States consists of more than 95,000 miles of coastline; 360 ports; 3.4 million square miles of Exclusive Economic Zones (EEZs); and thousands of bridges, dams, and levees. The task of protecting the MTS is enormous and essential to maintaining the security of the U.S. economy as shown by the following representative facts from 2008:²³

- 64 million passenger-nights were booked on North American cruises
- More than 4,200 cruises by the 17 largest cruise lines carried nearly 10 million passengers
- 147 million passengers traveled on ferries
- 7,100 commercial ships made approximately 60,000 U.S. port calls;
- U.S. foreign and domestic waterborne trade amounted to 2.3 billion metric tons
- 48 percent of U.S. foreign trade (imports/exports all modes) was moved by vessel in value terms, up from 41 percent five years earlier

2.2 Unique Characteristics of the Maritime Transportation Mode: Assets, Systems, and Networks

The MTS depends on and supports networks of critical infrastructure—both physical networks, such as the marine transportation system, and cyber networks, such as interlinked computerized operations and information-sharing systems. The ports, waterways, and shores of the maritime mode are lined with military facilities, nuclear power plants, locks, offshore oil and natural gas drilling and production platforms, oil refineries, levees, passenger terminals, fuel tanks, pipelines, chemical plants, tunnels, cargo terminals, underwater cable, and bridges. Collocated business infrastructure may also include restaurants, stadiums, or conference centers and create a publicly dense environment that poses numerous security and safety challenges that span the border between land and maritime jurisdictions.

The consequences of an incident, beyond immediate casualties, on one node of maritime critical infrastructure may include disruption of entire systems, congestion and limited capacity for product delivery, significant damage to the economy, or the inability to project military force. The protection of maritime infrastructure assets, systems, and networks must address individual elements, as well as intermodal aspects and their interdependencies positioned both within a regulatory environment and a system-of-systems.

Seaports and Marine Terminals

There are approximately 70 deep-draft port²⁴ areas along U.S. coasts, including approximately 40 that each handle 10 million tons or more of cargo per year. Within these ports are approximately 2,000 major terminals. Most of these terminals are owned by port authorities and are operated by the private sector. Marine terminals and their associated berths are often specialized to serve specific types of cargo or passenger movements. Terminals handling bulk cargo such as petroleum, coal, ore, and grain are frequently sited outside the boundaries of organized public port authorities. These facilities are often the origin and destination points for bulk commodities and, thus, they differ from terminals often found in public ports, where shipments are transferred from one mode to another. Terminals handling containerized cargo tend to be located within larger public port complexes with significant warehousing, storage, and intermodal transportation connectivity. Container terminals at 15 ports

²³ U.S. Department of Transportation, U.S. Water Transportation Statistical Snapshot, July 2009. Additional information is available from the Maritime Administration at <http://www.marad.dot.gov>.

²⁴ The Water Resources Development Act of 1986 defines deep-draft harbors as being authorized to be constructed to a depth of more than 45 feet. Additional information is available at <http://epw.senate.gov/wrda86.pdf>.

account for 85 percent of all container ship calls in the United States, and the port complexes in six geographic areas account for approximately 65 percent of these calls. These six areas are: Long Beach/Los Angeles, New York/Newark/Elizabeth, San Francisco/Oakland, Hampton Roads, Charleston/Savannah, and Seattle/Tacoma. Tanker calls are concentrated regionally in areas with significant petrochemical industries, such as the gulf coast, Delaware Bay, New York Harbor, San Francisco Bay, and San Pedro Harbor. The ports in southern Louisiana are the centers of dry bulk grain traffic, most of which moves down the Mississippi River for export on larger oceangoing ships.

Terminal Facilities

Hundreds of natural and manmade harbors are situated along the U.S. coastline and most contain federally maintained channels used regularly by both passenger and cargo vessels. Many piers and berths are privately operated and are designed to handle particular types of commodities. A terminal may be a stand-alone facility on the shoreline or part of a system of terminals and other marine service facilities (e.g., tugboat operators, fuel depots, ship repair facilities) that together make up a larger port complex. Individual terminals are often connected to rail sidings, roads that accommodate trucks, and pipelines. A terminal may be the origin or destination point for cargo moved on the waterways, as is the case for chemicals shipped from a waterfront chemical plant or coal shipped to the dock of a waterfront power plant.

Offshore Oil Facilities and Offshore Renewable Energy Installations (OREIs)

The EEZ contains offshore facilities used for U.S. crude oil and natural gas production. These facilities are a key component for the Energy Sector, located within the MTS. To reduce U.S. dependence on foreign energy supplies, alternative energy sources are being pursued; renewable energy sources such as OREIs are especially attractive. Often these techniques seek to exploit naturally occurring renewable sources such as solar, wind, and hydrodynamic energy. The United Kingdom and Denmark have emerged as leaders in the application of this technology and it is gaining popularity around the world.

In U.S. waters, the responsibility for permitting, approval, and oversight of OREIs is shared among a number of agencies, including the U.S. Department of the Interior (DOI) Minerals Management Service (MMS); the U.S. Army Corps of Engineers (USACE); the Federal Energy Regulatory Commission (FERC); the U.S. Departments of Commerce (DOC), Defense (DoD), Energy (DOE), and Transportation (DOT); and the U.S. Environmental Protection Agency (EPA). The appropriate State and tribal governments may also have interests depending upon the location of the OREI. MTS concerns with regard to the construction and location of an OREI are primarily related to the impact on navigation safety. Depending on the location, the OREI may affect commercial shipping, fishing, recreational boating, or other traditional uses on the waterway, or may cause interference affecting the performance of electronic navigation systems, including radar and communication systems. To mitigate these risks, safety zones, routing measures, and monitoring may be required.

Natural Gas Infrastructure

The majority of natural gas used in the U.S. is from domestic supplies; approximately 15 percent is imported, mostly by pipeline from Canada. A small percentage, approximately 1.5 to 3 percent of the total U.S. supply, comes from Liquefied Natural Gas (LNG) imported on specially designed LNG ships. Trinidad and Tobago, Algeria, and Egypt are the primary sources of imported LNG.²⁵ The majority of LNG imported into the U.S. is currently received at nine shoreside LNG facilities in operation in the U.S., including an import terminal in Puerto Rico. The remaining shoreside LNG facilities are located in Boston, MA; Cove Point, MD; Elba Island, GA; Lake Charles, LA; Cameron, LA; Sabine Pass, LA; Freeport, TX; and an export terminal in Kenai, Alaska. There are two operational deepwater ports (DWP) that import natural gas into the U.S. from special LNG ships designed to both carry and gasify LNG; the Gulf Gateway Energy Bridge DWP is located 116 miles off the coast of Louisiana and

²⁵ The Russian Federation, Norway, Qatar, and Republic of Yemen may become supply sources.

the Northeast Gateway Energy Bridge DWP is located approximately 20 miles off the coast of Boston. One additional DWP, the Neptune DWP, is planned to be operational in 2010; it is approximately seven miles off the coast of Gloucester, MA.

Navigation Infrastructure and Services

U.S. waterways consist of thousands of miles of main channels, connecting channels, and berths. The vast majority of U.S. maritime trade passes through the more than 300 deep-draft navigation projects that the USACE maintains nationwide. USACE's responsibility for inland waterways is complemented by the DOC National Oceanic and Atmospheric Administration's (NOAA) responsibility for coastal management; NOAA charts, preserves, enhances, and monitors the condition of the Nation's coastal resources and ecosystems. NOAA also manages the land, aerial, and orbital infrastructure supporting NOAA's development and issuance of marine weather forecasts, watches, and warnings. The USCG maintains nearly 50,000 aids to navigation, ranging from lighted buoys and beacons to radio navigation systems. Responsibility for waterways management includes coordinating and controlling vessel operations and scheduling on the waterways with Federal agencies, local pilot associations, private marine exchanges, port authorities, and individual vessel operators. Vessel navigation and related infrastructure and services are dependent on cyber- and communications-supported systems managed by various public and private owners and operators; these systems include Global Positioning Systems (GPS), Geographic Information Systems (GIS), Automatic Identification Systems (AIS), and Long-Range Identification and Tracking (LRIT). In addition, Vessel Traffic Services (VTS) provide the mariner with information related to the safe navigation of a waterway. This information contributes to the safe routing of vessels through congested waterways or waterways that contain a particular hazard. VTS Puget Sound is unique among the 12 VTS operated by the USCG. It is the only U.S. VTS that operates a cooperative international VTS with Canada. The Victoria (Canada), Tofino (Canada), and Seattle Traffic Centers coordinate shipping traffic between Puget Sound, the Straits of Georgia, Juan de Fuca, Rosario, Haro, and the west coast of Vancouver Island and northern Washington State out to 60 miles offshore.

Oceangoing Vessels

Major classes of oceangoing vessels are tankers, container ships, dry bulk and general cargo freighters, and specialized ships such as the roll-on/roll-off carriers used to transport motor vehicles. U.S. ocean ports and terminals handle more than 75,000 vessel calls per year. Tankers, container ships, and dry bulk carriers make about two-thirds of these calls.

Passenger Carriers

Many of the passenger vessels operating in U.S. territorial waters are ferries carrying automobiles, trucks, and passengers. Although they are an important part of the public transportation systems in cities such as Seattle, San Francisco, and New York, passenger ferries account for a small percentage of the Nation's total passenger trips on all public transportation modes, including subways and urban buses. Cruise ships continue to serve the recreation and tourism industries and operate on a regular basis from U.S. ports. An estimated 13.2 million travelers cruised in 2008, up from 12.56 million in 2007. The cruise industry also supports the economy. The cruise industry generated \$38 billion in total U.S. economic output in 2007 (the latest figures available), posting more than a 6 percent economic impact growth rate over 2006. Direct spending in the U.S. in 2007 on goods and services was more than \$18 billion, a 5.9 percent increase over 2006.²⁶

Inland River, Coastal, and Great Lakes Systems

Although the deep oceans are the primary means of moving cargo internationally, the U.S. inland river, coastal, and Great Lakes waterways are important means for moving cargo domestically and for providing outbound feeder traffic for overseas shipping:

²⁶ International Council of Cruise Lines, *Inside Cruising: A Guide for Travel Professionals*, <http://www.cruising.org/pressroom-research>.

- **Inland River Systems.** By far the largest and busiest inland waterway system in the U.S. is the Mississippi River system, which includes the large Ohio River and Missouri River tributaries. This system extends for more than 12,000 miles and encompasses navigable waterways on more than a dozen tributary systems passing through 17 States leading to the Gulf of Mexico. Barges are loaded and unloaded at shallow-draft terminals situated along the riverbanks. There are more than 1,800 shallow-draft terminal facilities in the U.S.
- **Coastal and Intracoastal Waterways.** The main coastal shipping activity in the U.S. occurs along the gulf coast and, to a lesser extent, along the Atlantic coast. The Gulf Intracoastal Waterway (GIWW), which is maintained by the USACE, spans 1,300 miles from Texas to Florida and is used for moving grain, coal, refinery products, and chemicals domestically and for supplying feeder traffic to seaports.
- **Great Lakes System.** Approximately 350 terminals are situated along the U.S. shoreline of the Great Lakes. A half-dozen lake ports, including Duluth–Superior, Chicago, Detroit, and Cleveland, rank among the top 50 U.S. ports in terms of tonnage. The terminals in these ports, as well as most others on the Great Lakes, primarily handle dry bulk cargo, led by iron ore, grain, coal, sand, stone, and lumber. During cooler seasons, icebreaking operations maintain maritime travel and trade routes and allow for the mobility of law enforcement, defense assets, and essential resources. Access to and transit within the Great Lakes system requires close international cooperation with Canada.

The Arctic System

An increased focus on the Arctic system and potential changes to the MTS has emerged due to climate change. The majority of Arctic shipping is destination specific; although there were a few trans-Arctic voyages in 2008. The character of shipping in the Arctic is likely to remain similar for some time. There is considerable fishing activity in the Bering Sea and the Arctic Marine Shipping Assessment 2009 Report²⁷ found that of the approximately 6,000 vessels in the Arctic in 2004, nearly half were operating on the Great Circle Route, which crosses the Aleutian Islands and the southern Bering Sea. Due to the geography and country boundaries, the U.S. Government maintains a positive working relationship with MTS counterparts in Canada and the Russian Federation. The U.S. Arctic from the Bering Strait northward, at present time, lacks the infrastructure to support the MTS beyond its current demand.

Defense Port and Facility Prioritization

DoD may require priority use of commercial port and intermodal facilities and services to meet military deployment or other defense emergency requirements. Pursuant to the Defense Production Act of 1950, the Maritime Administration (MARAD) has authority (46 Code of Federal Regulations (CFR) 340), delegated from the Secretary of Transportation, to require priority use of commercial port facilities and services by DoD ahead of commercial port contractual obligations. MARAD also has in place standby Federal Port Controller (FPC) service agreements (46 CFR 346) with key executives at 15 U.S. ports. Each FPC is responsible for prioritizing and controlling the utilization of port facilities, equipment, and services to ensure that military deployment cargo movement timelines are met, while minimizing congestion and disruption to the movement of commercial cargo.

The National Port Readiness Network (NPRN) helps prepare port and DoD personnel to use relevant emergency procedures and coordinates deployments through ports. NPRN comprises ten Federal agencies (MARAD, U.S. Transportation Command, USCG, the Transportation Security Administration, U.S. Northern Command, Surface Deployment and Distribution Command, USACE, U.S. Army Forces Command, Military Sealift Command, and U.S. Army Installation Management Command) with missions supporting the secure movement of military cargo during deployments or other national emergencies. Training and coordination are accomplished through the local NPRN Port Readiness Committees.

²⁷ Arctic Council, Arctic Marine Shipping Assessment 2009 Report, 2nd printing, April 2009, p. 91.

Maritime Security Levels

The USCG has a three-tiered system of MARSEC levels to reflect the prevailing threat environment to the maritime elements of the national transportation system. MARSEC levels are designed to provide a means to easily communicate pre-planned scalable responses to increased threat levels.²⁸ Level 1 indicates the level for which minimum appropriate security measures shall be maintained at all times and generally corresponds to DHS Homeland Security Advisory System (HSAS) Threat Condition Green, Blue, or Yellow. Level 2 indicates the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of a heightened risk of a TSI and generally corresponds to HSAS Threat Condition Orange. Level 3 indicates the level for which specific protective security measures shall be maintained for a limited period of time when a TSI is probable, imminent or has occurred, although it may not be possible to identify the specific target and generally corresponds to HSAS Threat Condition Red. The Commandant of the USCG sets MARSEC levels, but because of the unique nature of the maritime industry, MARSEC levels will align closely with HSAS Threat Conditions but will not directly correlate.²⁹ The international community also uses a three-tiered advisory system specified by the International Ship and Port Facility Security (ISPS) Code.³⁰ MARSEC levels are consistent with the international three-tiered advisory system. A further description of and discussion on the application of MARSEC levels is appendix D.

Figure B2-1: Maritime Security Levels



Intermodal and Cross-Sector Connections

Intermodal transportation refers to a system that connects the separate transportation modes, such as aviation, maritime, mass transit, highway and motor carrier, pipelines, and freight rail, and allows a passenger or cargo to complete a journey using

²⁸ See <http://www.uscg.mil/safetylevels/whatismarsec.asp> for additional information.

²⁹ Maritime Security Directives are instructions issued by the Commandant, USCG, or designee, mandating specific security measures for vessel and facilities.

³⁰ Information on security levels 1, 2, and 3 can be found in the ISPS Code and SOLAS Chapter XI-2.

more than one mode. In terms of cargo transportation, an intermodal shipment is generally one that moves by two or more modes during a single trip. Intermodal connections link the various transportation modes—maritime ports and related facilities, highways, rail, and air. Sector overlaps occur due to the dynamics of the environment. For example, the Energy Sector and the Communications Sector connect through pipelines and underground cable that are part of the MTS. In another example, bridges and tunnels provide pathways for pipelines, mass transit, and railroads. A wide range of interconnected cyber assets reinforce, and can complicate, the interdependencies within the sector. Many cyber systems, such as control systems or data centers, are shared between multiple transportation entities. Cyber attacks or other events disrupting these systems could have extended consequences for owners and operators across multiple modes. Furthermore, commodities are shipped through multiple modes that depend on one another for timely and secure deliveries to customers. These modal interdependencies require special consideration of the potential consequences from the cascading effects of an incident and for informing short-term recovery to restore partial functionality and as a precursor to such long-term recovery measures and activities as may be necessary to return to a steady-state condition, adapted to whatever changes that may be outcomes from an incident.

Transportation Worker Identification Credentialing (TWIC)³¹

Implementation and enforcement of TWIC is well underway with nearly 1.3 million American workers carrying a uniform credential in U.S. ports by the end of 2009. These tamper-resistant, biometric credentials are issued to workers who require unescorted access to secure areas of ports, vessels, and outer continental shelf facilities, and to U.S.-credentialed merchant mariners.

2.3 Risk Considerations

Risk is the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.³² Due to the layered complexity of the MTS, it is susceptible to risks posed by all hazards across the physical, cyber, and human risk elements. These hazards can occur simultaneously within the maritime domain. Threats and hazards such as flooding, hurricanes, and pandemics, and risks posed by aging infrastructure have advance warning indicators; other events are less predictable, such as earthquakes and tornadoes. Systemic neglect of infrastructure may cause a failure of critical assets, presenting a hazard to the resilience of the MTS. The prediction of human behaviors can be relatively challenging; human action, either intentional or unintentional, could result in a major accident or incident with catastrophic consequences.³³ The deliberate actions of malicious actors may cause damage or impede response efforts. The distinctions between terrorism and criminal activities will most likely continue to blur as extremist groups attempt to support their objectives through other criminal enterprises by attempting to blend into the course of legitimate activity.

The Physical Risk Element

Utilizing best practices and lessons learned, partners within the maritime environment continue to enhance their operating plans and procedures to prepare for, respond to, and recover from all-hazard events, thereby improving the resilience of the Nation's MTS. Hurricanes, tornados, and flooding are examples of natural disasters that typically cause significant disruption to the MTS. The improved preparation, response, and recovery measures and actions to significant events were apparent in the resilience demonstrated in the wake of hurricanes Gustav and Ike in 2008. Aging infrastructure also poses a risk; the collapse of an I-35 Mississippi River bridge in Minneapolis in 2007 alerted and raised public consciousness of the risk. A similar incident could disrupt the supply chain and potentially have negative psychological consequences that could result in a cascading negative economic impact.

³¹ TWIC was established by U.S. Congress through MTSA; it is administered by both TSA and the USCG.

³² National Infrastructure Protection Plan, p. 111.

³³ Consequences can be divided into four main categories: public health and safety, economic, psychological, and governance impacts (National Infrastructure Protection Plan, p. 109).

Threats posed in the physical risk element are diverse. The worst-case threat scenario is the introduction of nuclear, biological, or chemical weapons or radiological dispersal devices, while the use of improvised explosive devices (IEDs) remains the most likely tactic for terrorist attacks against transportation systems worldwide. Another area of great concern is the misuse of cargo containers for human and weapons trafficking, transporting counterfeit goods, and improper labeling of hazardous materials and other goods. Cruise ships and supertankers continue to increase in size, and this poses a global challenge for safety and security, including environmental and other impacts.

The Cyber Risk Element

Cyber exploitation by malicious actors, including terrorists, poses a risk to critical infrastructure. The Nation's information infrastructure, including systems, networks, and data, must be understood and prioritized, protected, and made resilient. Incidents must be managed from identification to resolution in a rapid and replicable manner.

Unlike physical infrastructure assets, cyber assets are not necessarily found in a specific physical location and, therefore, the risk methodology used to identify high-value physical assets cannot necessarily be applied. Incorporating cyber threat scenarios to identify risk in a particular supply chain or system that transcends both the virtual and physical realms, be it at a local, regional, national, or international level is a challenging undertaking. Identification of a cyber system alone, does not necessarily provide significant value; it is the dependency and interdependency of the system and the cascade of consequences that provide greater value. For example, the supply chains of almost all other functions and systems are dependent on the Nation's transportation networks and these systems are becoming more and more enabled through cyber systems and services. If the transportation networks fail, almost every major economic, social, and government service may experience cascading negative effects. The Nation's critical infrastructure sectors rely extensively on information technology systems,³⁴ systems that in and of themselves may be critical. The inability to restore electronic information and communications systems in the event of a terrorist attack or natural disaster poses another risk.

Cyber exploitation activities continue to become increasingly sophisticated and dependencies and interdependencies among cyber systems can be difficult to identify. Assets can be physical, such as computer hardware, but can also exist entirely in the virtual realm making them more difficult to pinpoint and secure. As is the case with most CIKR sectors, the MTS is dependent on information assurance and the ability to securely process, store, and distribute electronic information. Cyber intrusions occur on a daily basis around the world; the greatest threat to the MTS is the intrusion of cyber control systems, which consist of computer-based programs that operate motors, pumps, valves, signals, lighting, and access controls. For example, cyber control systems operate heating and cooling systems, security access control systems, collision avoidance systems, GIS tracking systems, and fire suppression systems. The exploitation or degradation of cyber systems may coincide with a natural disaster or deliberate attack and could result in cross-sector system failures. Cyber system failures can degrade or interrupt the operation of transportation services. The level of risk depends on the degree to which a service relies on the infrastructure's cyber component and on the potentially cascading effects that a cyber event may trigger.

The Human Risk Element

Human risk elements are familiar to the MTS and the seafarer. Factors, such as credentialing, workplace standards and training, and physiological well-being affect the ability of the transportation worker to remain alert, identify anomalies, and reduce complacency. More than 80 percent of the world's trade depends on the professionalism and competence of seafarers.³⁵ The human element is a complex multidimensional issue impacting maritime safety, security, and marine environmental protection and involves the entire spectrum of human activities performed by ship crews, shore-based management, regulatory bodies,

³⁴ Government Accountability Office, Critical Infrastructure Protection: Current Cyber Sector-Specific Planning Approach Needs Reassessment, Report No. GAO-09-969.

³⁵ See <http://www.imo.org> for more information.

and others. The lack of a dynamic workforce capable of cyber innovation is a concern for both the public and private sectors. Another workforce concern is that the MTS is vulnerable to deliberate or inadvertent actions by transportation system workers that may threaten high-consequence assets. The dynamic tempo of operations and the influence of environmental factors can contribute to accidents and errors that can lead to catastrophic results; there is human risk in both errors of judgment and malicious intent. Regulatory and non-regulatory public-private partnerships are keys to reducing these risks. The human risk element also includes consequences of public health and safety, such as pandemic threats; the H1N1 event in 2009 is such an example.

2.4 Framework for Partnership and Information Sharing

Information-Sharing Policy and Authorities

Information-sharing processes are in use between the government and the private sector; these legacy mechanisms are often guided by regulation, precedent, or established process. In 2009, a Presidential Memorandum for the heads of executive departments and agencies was issued in support of transparency and open government, specifically that government should be transparent, participatory, and collaborative; this memorandum was also published in the Federal Register.³⁶

Federal Coordination with State, Local, and Tribal Governments

Coordination with State, local, and tribal officials occurs on an ongoing basis; the enhancement of these mechanisms to be relevant and timely is a priority of DHS and impacts risk reduction activities and the resilience of the maritime domain. A Presidential Memorandum on Tribal Consultation³⁷ recently emphasized the importance of consultation with tribal officials as a critical ingredient of sound and productive Federal-tribal relationships. Increasingly, technology serves a predominant role in the mechanics of sharing information and collaboration. However, the efficiency of process and the value of effort must be balanced; preventing an undue burden and adhering to the Paperwork Reduction Act of 1995, the Federal Advisory Committee Act, and the Critical Infrastructure Partnership Advisory Council (CIPAC) exemption as exercised under section 871 of the Homeland Security Act of 2002 are important considerations. Existing mechanisms for sharing information include Information Sharing and Analysis Centers (ISACs), Homeport, Area Maritime Security Committees (AMSCs),³⁸ Port Readiness Committees, Carrier and Trade Support Groups,³⁹ the U.S. Computer Emergency Readiness Team (US-CERT), the Homeland Security Intelligence Network-Critical Sectors (HSIN-CS), and the Common Assessment and Reporting Tool (CART) and are discussed briefly below.

Information Sharing and Analysis Centers (ISACs)⁴⁰

The Maritime ISAC is unique from other CIKR ISACs in that it is not managed by the private sector, but by the USCG Office of Port and Facility Activities. It facilitates the sharing of security, critical infrastructure, and threat information with government and industry maritime security and critical infrastructure partners. Currently, the primary function of the Maritime ISAC is to serve as the focal point for gathering and disseminating information regarding maritime threats to interested stakeholders.

³⁶ The White House, Memorandum on Transparency and Open Government, 2009, http://www.whitehouse.gov/the_press_office/transparencyandopengovernment.

³⁷ The White House, Memorandum on Tribal Consultation, 2009, <http://www.whitehouse.gov/the-press-office/memorandum-tribal-consultation-signed-president>.

³⁸ Maritime Security Preparedness relies on Area Contingency Plans and Area Committees to address response and mitigation from releases of oil or hazardous materials into the marine environment.

³⁹ Under the CBP/USCG Joint Protocols for Expeditious Resumption of Trade.

⁴⁰ In 2003, under industry advisement, the Maritime ISAC was formed; it is facilitated by the Office of Port and Facility Activities at USCG Headquarters in Washington, D.C.

The Maritime ISAC operates at the national, regional, and local levels and provides information on risks to the MTS, as well as information concerning incidents, threats, attacks, vulnerabilities, and potential consequences. The Maritime ISAC also processes and analyzes incoming information in terms of which maritime stakeholder groups need the information and disseminates threat warning products to maritime stakeholders in a timely manner; enables the maritime community to identify, report, and share information to reduce security vulnerabilities; and facilitates the discussion and development of best practices and solutions on subsector and cross-sector issues between public and private sector stakeholders. The Maritime ISAC draws from multiple information sources from the national to the local levels of the public and private sectors. Currently, the Maritime ISAC leverages the technology of Homeport as an organized mechanism for the secure exchange, dissemination, coordination, and storage of sensitive information.

Providing a two-way information-sharing process between maritime industry stakeholders and the government is under consideration for future development within the construct of the Maritime ISAC. Overall, the Maritime ISAC assists the maritime industry and State and local agencies with strengthening the Nation's capabilities to prevent, detect, respond to, and recover from potential TSIs on the MTS.

Homeport⁴¹

Homeport is a publicly accessed and secure enterprise Internet portal that supports port security functionality for operational use. It also serves as the USCG's primary communications tool to support the sharing, collection, and dissemination of Sensitive But Unclassified (SBU) information, including Sensitive Security Information (SSI), For Official Use Only (FOUO), and Law Enforcement Sensitive (LES) information.

Homeport meets critical information-sharing mission requirements in support of MTSA and is used as a primary means for day-to-day management and communication of port security matters between public and private stakeholders from the national to the local levels, including coordination and collaboration between Federal Maritime Security Coordinators (FMSCs) and AMSC members, commercial vessel and facility owners and operators, government partners, and the public. Homeport includes the Alert Warning System (AWS) function, which provides time-sensitive status updates (e.g., MARSEC level changes).

Area Maritime Security Committees (AMSCs)

MTSA mandated the development of a new regulatory scheme for maritime security that set forth requirements to establish the AMSCs;⁴² 43 AMSCs are now active at the local port level and are instrumental in achieving and sustaining a robust maritime security regime to protect the Nation's MTS. The purpose of the AMSCs is to assist and advise the COTP (acting as the FMSC) with the development and maintenance of the Area Maritime Security Plan (AMSP) by providing a framework to communicate, identify risks, and coordinate resources among key port stakeholders to mitigate threats and consequences within the area of responsibility (AOR). AMSCs contribute to the establishment of a Maritime Common Operating Picture (MCOP) that permits decisionmakers to access critical and time-sensitive information. AMSCs provide a vital link for contingency planning and collaboration between Federal, State, local, law enforcement, and industry partners and are a cornerstone of U.S. national maritime security.

Maritime Government and Sector Coordinating Councils

In 2006, the MMGCC stood up as a subsector of the Transportation Systems Sector Government Coordinating Council (GCC). Primary membership consists of representatives from DHS, DOT, DoD, DOC, and the U.S. Department of Justice (DOJ). The responsibilities of the MMGCC are derived from the NIPP and the charter of the Transportation Systems Sector GCC. The

⁴¹ Additional information on Homeport is available at <http://homeport.uscg.mil>.

⁴² The regulation creating AMSCs is contained within 33 CFR 103.300. It implements that portion of the MTSA found at 46 U.S.C.A. 70112.

Maritime Modal Sector Coordinating Council (MMSCC) stood up in 2007; membership consists of owners, operators, and associations from within the sector. The modal GCC and Sector Coordinating Council (SCC) may also participate in Homeland Security Presidential Directive 7 (HSPD-7)-designated CIKR sector working groups, such as cyber, metrics or research and development. The SSA, other Federal agencies, industry, and the public sector have an extensive history of collaboration in meeting the various safety and security needs, many of which pre-date the CIPAC Partnership Model. The formation of the MMGCC and MMSCC do not replace these existing mechanisms, but instead complement them, and scope specifically toward the protection of critical infrastructure in the MTS.

Homeland Security Intelligence Network–Critical Sectors (HSIN-CS)

HSIN-CS is a Web-based platform developed by DHS created to support information sharing and collaboration between Federal, State, local, tribal, private sector, and international partners engaged in preventing, protecting from, responding to, and recovering from all threats, hazards, and incidents within the U.S. HSIN-CS facilitates collaboration between mission areas such as Law Enforcement, Emergency Management, and Critical Sectors within the various States, Territories, the National Capital Region, and major urban areas. The CIKR sectors utilize HSIN-CS to share information among modal partners just prior to, during, and after an incident. HSIN-CS augments the maritime stakeholder's primary information sharing portal Homeport and has been useful in sharing cross-sector CIKR information during all-hazard events.

National Infrastructure Coordinating Center (NICC)

The NICC is a 24/7 watch/operations center and Incident Management Cell that maintains ongoing operational and situational awareness of the Nation's CIKR sectors. The NICC is the CIKR-focused element of the National Operations Center, providing a centralized mechanism and process for information sharing and coordination between the government, the SCCs, the GCCs, and other industry partners. The NICC receives and shares situational, operational, and incident information in accordance with the information-sharing protocols established in the NIPP and the National Response Framework (NRF). The NICC posts updated CIKR sector information daily on HSIN-CS.

National Maritime Intelligence Center (NMIC)

The National Maritime Intelligence Center, established in 2009 to integrate and optimize the Global Maritime Community of Interest (GMCOI), integrates the unique capabilities of interagency, private sector, and foreign partners. On behalf of the GMCOI, the NMIC closes analytic and collection gaps, delivers interagency collaboration and information sharing solutions, advises interagency policy development, researches, and evaluates emerging technologies.

Common Assessment and Reporting Tool (CART)⁴³

CART is used to report, share, and track MTS impacts during an all-hazard incident that significantly disrupts the MTS in U.S. ports. CART provides an inventory of MTS baseline data that is based on 22 Essential Elements of Information (EEI). The CART database provides a repository of MTS recovery information that is not otherwise available to Federal, State, local, and tribal government officials. See section 3 for amplifying information.

U.S. Computer Emergency Readiness Team (US-CERT)

US-CERT is the operational arm of the DHS National Cyber Security Division (NCSD). The NCSD serves as the Federal Government's cornerstone for cybersecurity coordination and preparedness, including implementation of the National Strategy to Secure Cyberspace. US-CERT provides response support and defense against cyber attacks for the Federal Civil Executive

⁴³ CART is pending an adaptation into the enterprise system; field application continues.

Branch and provides information sharing and collaboration with Federal, State, and local government; industry; the research community; and international partners. US-CERT also provides a way for citizens, businesses, and other institutions to communicate and coordinate directly with the U.S. Government about cybersecurity.⁴⁴ The USCG shares cyber-related information with US-CERT regarding threats and attacks conducted against SSA assets. CIKR partners, especially owners and operators, are encouraged to use this same reporting mechanism in order to limit the consequences and diminish the vulnerabilities the sector faces with regard to cyber attacks.

⁴⁴ Additional information on US-CERT is available at <http://www.us-cert.gov>.

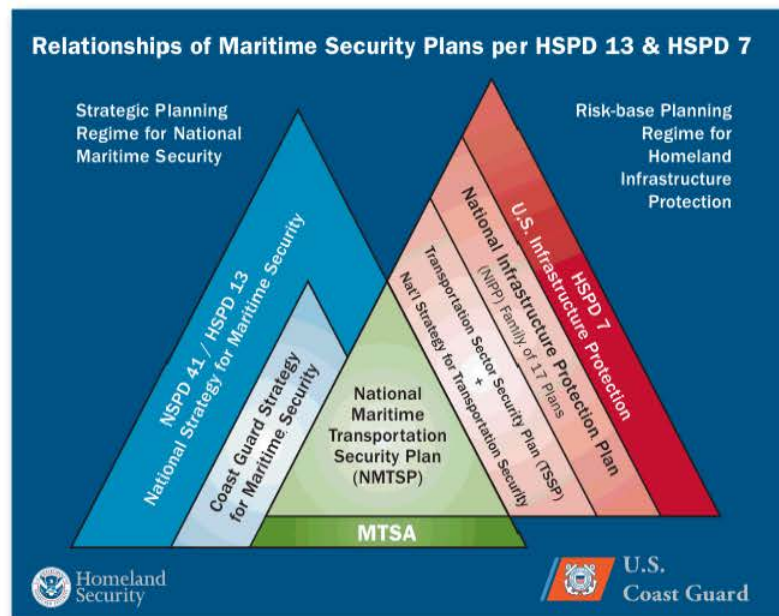
3. The Implementation Plan

Both the strategic planning regime for national maritime security and the risk-based planning regime for homeland infrastructure protection integrate to form a risk-based plan focused on protecting the public and managing security risks posed to assets and infrastructure within the maritime domain. Figure 3-1 is a representative example of the concurrent implementation of three Federal security requirements.⁴⁵

National Maritime Security Policy and Risk-Based Planning

The strategic planning regime for national maritime security and the risk-based planning regime for homeland infrastructure protection are depicted below. National Security Presidential Directive 41 (NSPD-41)/HSPD-13 guide the NSMS and its eight supporting plans, it should be noted that HSPD-7 guides U.S. infrastructure protection and the NIPP to build a safer, more secure, and more resilient America using the NIPP risk management framework across physical, cyber, and human risk elements. Transportation Systems Sector and maritime modal partners work together toward this aim, focusing on preparedness, response, and rapid recovery in the event of an attack, natural disaster, or other emergency.

Figure B3-1: Relationship of Maritime Security Plans per HSPD-13 and HSPD-7



⁴⁵ While this example uses the USCG as the implementing agency, it is serving as a proxy for all Federal security partners.

The NMTSP implements ten statutory requirements of the MTSA and creates a three-tiered maritime security planning regime, which includes AMSPs, along with vessel and facility security plans. The process to re-establish cargo flow after a maritime TSI aligns with NSPD-41/HSPD-13, as well as the Maritime Infrastructure Recovery Plan, to protect the economy of the United States by ensuring the continuity of maritime commerce and the MTS following a maritime TSI. Both of these plans protect the U.S. CIKR system using risk-based decisionmaking in close cooperation with State, local, tribal, and private sector partners.

3.1 Vision, Goals, and Objectives ⁴⁶

The security of the maritime domain is the collective effort of public and private sector owners and operators. While stakeholders, in general, share and support Transportation Systems Sector goals, each pursues these goals in accordance with its own requirements (e.g., business, mission, executive, or legislative). Government security partners execute their responsibilities either individually or as part of a larger collaborative effort by enforcing Federal regulation, programs, plans, and strategies. These cumulative activities implement the responsibilities of the partners, which include, but are not limited to, the protection of CIKR.

The vision, goals, and objectives of the maritime transportation mode are:

Vision Statement Maritime Transportation Mode

Through partnering, sustain a secure and efficient MTS that enables legitimate travelers and goods to move without fear of harm, reduction of civil liberties, or disruption of commerce.

Goal 1: Prevent and deter acts of terrorism using, or against, the MTS.

Objectives

- Continue to develop and implement flexible, layered security measures, both routine and random, while increasing security awareness training and security information sharing.
- Conduct and/or participate in combined drills and exercises to test, practice, and evaluate the execution of prevention/protection operations and contingency plans and procedures.

Goal 2: Enhance the all-hazard preparedness and resilience of the MTS to safeguard U.S. national interests.

Objectives

- Reduce the risks associated with key nodes, links, and flows within critical MTS areas to enhance overall MTS survivability and will continue to develop flexible contingency plans that are exercised and updated to ensure the most expeditious response and recovery to all-hazard events.
- Identify physical, cyber, and human risk elements in relation to the protection of the MTS.
- Improve cross-modal, cross-sector, and international coordination to address critical dependencies and interdependencies; incorporate into the risk management framework.
- Determine critical cyber assets, systems, and networks; identify and implement measures to address strategic cybersecurity priorities; and develop new and/or enhance existing maritime modal processes.

⁴⁶ See Transportation Systems SSP Base Plan for Transportation Systems Sector goals; these goals are supported by the mode where appropriate. These goals also support the national goals contained in the NSMS.

Goal 3: Maximize cost-effectiveness for the limited resources of the MTS.⁴⁷

Objectives

- Align resources to MTS security risks by priority and develop and disseminate standards for risk analysis tools and methodologies.
- Coordinate Federal, State, and local government agency efforts for maritime safety and security improvement and minimize the duplication of agency efforts.

Goal 4: Contribute to the improvement of sector situational awareness, understanding, and collaboration.

Objectives

- Enhance timely information sharing among MTS partners, as appropriate.
- Advance resiliency concepts and risk management best practices within the mode.
- Understand modal, intermodal, and cross-sector interdependencies, and collaborate with security partners through plans, training, and exercises to enhance knowledge.

3.2 Strategic Risk in the MTS

A strategic risk may be described as risks which impacts the entire Transportation Systems Sector and has consequences with far-reaching, long-term effects on the national economy, natural environment, and public confidence. The consequences of strategic risks generally cross multiple sectors. The risk management framework will inform decisionmakers at all levels and will be particularly relevant prior to, during, or after a strategic risk event.

As described previously, the MTS depends on networks of critical infrastructure, both physical and cyber. The port waterways and shores of the maritime mode are collocated with military facilities, nuclear power plants, locks, oil refineries, levees, passenger terminals, fuel tanks, pipelines, chemical plants, tunnels, cargo terminals, underwater cables, and bridges. Ports, in particular, have inherent security vulnerabilities and are sprawling, easily accessible by water and land, close to crowded metropolitan areas, and interwoven with complex transportation networks. Port facilities, along with the ships and barges that transit port waterways, are especially vulnerable to tampering, theft, and unauthorized entry.

Some physical and cyber assets, as well as associated infrastructure, also function as defense critical infrastructure; their availability is consistently ensured for national security operations worldwide. Just-in-time methods, utilized by industries, are considered for their implications for risk vulnerability. Beyond the immediate casualties, the consequences of an incident on one node of maritime critical infrastructure may include the disruption of entire systems, congestion and limited capacity for product delivery, significant damage to the economy, or an inability to project military force. The protection of maritime infrastructure networks must address individual elements, as well as intermodal aspects and their interdependencies positioned both within a regulatory environment and a system-of-systems.

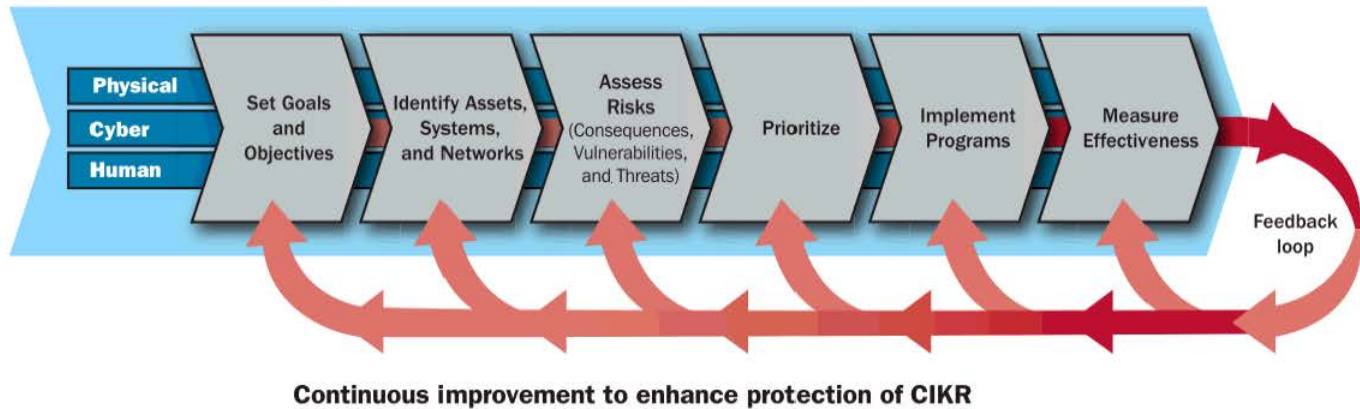
The SSA participates in the annual prioritization of Level 1 and Level 2 assets, and in the Critical Foreign Dependencies Initiative through the National Critical Infrastructure Prioritization Program, which fulfills the requirements of the Implementing Recommendations of the 9/11 Commission Act to produce lists of infrastructure that if disrupted could cause nationally or regionally catastrophic effects.

⁴⁷ To the greatest extent possible under the law.

3.3 Assessing Risk and Prioritizing Assets and Systems: Tactical/Operational Risk Planning

By applying the NIPP risk management framework, security partners within the maritime mode will continue to establish the processes for combining threat, vulnerability, and consequence information to produce a comprehensive systematic and rational assessment of the MTS, thereby also contributing to the overall risk management framework for the Nation.

Figure B3-2: NIPP Risk Management Framework



Effective Tools for Risk Management and Prioritization

The primary tool used to assess risk to national infrastructure in the maritime domain is MSRAM, which is used extensively at the local, regional, and national levels. The USCG and other maritime industry stakeholders use MSRAM to analyze strategic, operational, and tactical risks within and across U.S. ports. It allows risk managers and decisionmakers to understand the geographic density of risk across the Nation's ports, know the profile of risk within a port, and recognize asset-specific risks to help identify maritime CIKR assets. The tool is designed to allow a port-level user to assess the risk factors associated with a target (asset) in the maritime domain in such a way that local data can be used for both local and national risk analysis needs and can be fed into the overall risk management process. MSRAM is built on the standard risk formula where $\text{Risk} = f(\text{Threat} \times \text{Vulnerability} \times \text{Consequence})$ and encourages not only point-source protective measures, but also areawide security measures and response capabilities. As our understanding of risk has matured, broader systems assessment data now is incorporated into MSRAM. Although cyber risk data is contained, it is expected that the understanding of cyber risk and how it relates to the broader system will further evolve.

As previously discussed, CART is used to report, share, and track the impacts on the MTS during an all-hazard incident that significantly disrupts the MTS in U.S. ports. The information contained in CART assists decisionmakers with (1) facilitating MTS recovery operations vis-à-vis providing timely and accurate information on pre-incident conditions in a COTP zone, (2) comparing baseline MTS data and post-incident data to characterize the extent of the impact on the MTS, and (3) auto-generating an MTS Executive Summary for the sharing of findings with MTS stakeholders and port partners in a Web-based format to facilitate distribution and timely information sharing of MTS recovery status and impact reports.

Operational Risk Planning

From a system-of-systems perspective, the MTS is a network of maritime operations that interface with shoreside operations at intermodal connections as part of the overall global supply chain or domestic commercial operations. The various operations within the MTS network have components that include vessels, port facilities, waterways and waterway infrastructure, intermodal connections, and users. The United States, like many other nations, works toward maintaining a balance between safe, secure ports and facilitating trade that promotes economic growth and prosperity. The USCG Strategy for Maritime Safety,

Security, and Stewardship; the PWCS mission; and the CMT Performance Plan are efforts to guide this balance between safe, secure ports and economic prosperity. Efforts to safeguard the Nation's interests are best understood when viewed as part of a larger interlocking system of governance comprised of operational capabilities, domain awareness, and maritime regimes applied across the maritime domain. Layered security has geographic and functional aspects; boundaries in terms of the geographic layer or zone where operations will be conducted (e.g., domestic, border/coastal, or an international zone); and functional aspects of operations that unify regional and global efforts to counter terrorism and other illicit activity.

3.4 Decisionmaking Factors

The CIKR within the maritime transportation mode constitute a vital part of the complex systems necessary for public well-being, as well as economic and national security. They are essential for the free movement of passengers and goods throughout the world. Many factors influence decisionmakers when it comes to conducting risk mitigation activities across physical, cyber, and human elements. Among these factors are executive mandates, legislative mandates, leadership priorities, budget constraints, time requirements, and risk assessments. National priorities drive decisionmaking at a strategic level.

The national-level risk management framework is applicable to risk assessment on an asset, system, network, functional, national, State, regional, or sector basis. Maritime partners contribute to the national-level risk management framework through various mechanisms and multiple interface points. For example, owners and operators may identify assets, systems, networks, and functions at a local level, and national-level advisory councils may provide recommendations on the priority and implementation effectiveness of particular protective programs, while other subject matter experts may provide valuable scenario-building knowledge. The risk management framework in the MTS is both a bottom-up build and a top-down build, combined with cross-sector integration.

MTS security partners derive their responsibilities and priorities, both individually and collectively, from several main sources, including international agreements, treaties and conventions, legislation, executive directives, and assigned mission(s).

Public and private sector security partners have worked collaboratively to execute these responsibilities to create a layered security regime. This layered regime includes the International Maritime Organization's ISPS Code, championed by the U.S. and other contracting governments. The ISPS Code has been implemented and is monitored by the U.S. and other member states around the world. The MTSA, developed contemporaneously with the ISPS Code, implements security requirements for the U.S. maritime industry. Government partners execute their responsibilities by enforcing Federal regulations, programs, plans, and strategies. These cumulative activities implement the responsibilities of the partners, which include, but are not limited to, the enhanced protection of CIKR through the NIPP sector partnership model, the NIPP risk management framework, and complementary RMAs.

The Level 1, Level 2, and sector lists are utilized during incidents as a valuable tool for prioritizing Federal, State, and local response and recovery efforts. Specifically, the USCG, as the SSA, uses its MSRAM tool to identify maritime, national-level CIKR assets and systems. MSRAM was designed to incorporate all 18 CIKR sectors and, therefore, has application beyond assets and systems that are maritime centric; presently, 13 of the 18 CIKR sectors are represented and have data in the MSRAM tool. Prior to and during an event, the SSA, as the subject matter expert, is often consulted by other CIKR sectors, adding redundancy to their existing mechanisms. This data is readily available and repeatable, but due to the complexity, may require subject matter expertise to interpret the findings in context with a particular event or scenario. Analysis is performed and provided in a format that the end user can utilize, along with other tools and subject matter expertise, to inform decisions.

Domain Awareness is a key enabler of continuous risk identification and subsequent resource prioritization and allocation decision support. The steady-state Domain Awareness is typically provided via an operations center environment is essential to all-hazard incident prevention and includes a situational awareness aspect that is essential to incident management of small-scale, short-term, and non resource-intensive operational activities.

The incident management of large-scale, long-term, and resource-intensive operational activities typically overloads the all-hazard risk identification capability of the steady-state domain awareness-focused operations center. This overload effect requires a new “incident defined” domain that is either geographic or functional in nature and enables the start-up of a separately staffed management team with a refined situational awareness focus. This refined situational awareness and subsequent incident management staffing requirement pertains to potential or actual large-scale operational activities. From the national to the local level, executive agents, security partners, operations centers, incident-driven Unified Command start-ups, and decisionmakers must have steady-state domain awareness to be able to transition to accommodate refined situational awareness in order to implement effective incident prevention, response, and recovery protocols.

3.5 Programs, Initiatives, and Risk Mitigation Activities

The chart below shows a representative breadth of program initiatives and other activities that support the maritime mode's RMAs. Information-sharing programs and activities cascade across all four RMAs. The RMAs identified by the mode include the following:

- Risk Reduction Tools and Methods
- Lead and Conduct Effective Maritime Security and Response Operations
- Maritime Domain Awareness
- Create and Oversee an Effective Maritime Security Regime

These RMAs contribute to the reduction of risk in the maritime domain across physical, cyber, and human risk elements; they are linked to the goals identified in section 3.1. The programs and initiatives may also support other areas within their multi-mission agencies and respective departments.

Risk Reduction Tools and Methods

Department/Agency	MTS Program/Initiative * Denotes Key RMA	Maritime Goal Supported	Element (Physical, Cyber, Human)
DHS/CBP	Canine Enforcement Program	1	Physical
DHS/CBP	Non-Intrusive Inspection Technology (NII)	1	Physical
DHS/FEMA/USCG	* Discretionary Transportation and Infrastructure Security Grants, Port Security Grant Program (PSGP)	1, 2, 3, 4	Physical, Cyber, Human
DHS/TSA	Intermodal Security Training and Exercise Program (I-STEP)	1, 2, 4	Physical, Human
DHS/TSA	Security Enhancement and Capability Augmentation Program (SEACAP)	1	Physical
DHS/TSA	Security Training, Operational Readiness, and Maritime Community Awareness Program (STORMCAP)	1, 4	Physical, Human
DHS/USCG	Area Maritime Security Training and Exercise Program (AMSTEP)	1, 2, 4	Physical, Human

Department/Agency	MTS Program/Initiative * Denotes Key RMA	Maritime Goal Supported	Element (Physical, Cyber, Human)
DHS/USCG	Maritime Force Protection Units (MFPUs), Transit Protection System (TPS)	1, 2	Physical
DHS/USCG	* Maritime Security Risk Analysis Model (MSRAM)	1, 2, 3, 4	Physical
DHS/USCG	National Maritime Terrorism Threat Assessment (NMTTA)	1	Physical, Human
DHS/USCG	Port Threat Assessments	1, 2, 3	Physical

Lead and Conduct Effective Maritime Security and Response Operations

Department/Agency	MTS Program/Initiative * Denotes Key RMA	Maritime Goal Supported	Element (Physical, Cyber, Human)
DHS	Protective Security Advisors	1, 2, 4	Physical, Cyber, Human
DHS/CBP/ICE/USCG	CBP, USCG, and Immigration and Customs Enforcement (ICE) Senior Guidance Team (SGT)	4	Physical, Human
DHS/CBP/USCG	CBP/USCG Dual-Agency Boarding Initiative	1, 4	Physical, Human
DHS/CBP/USCG	National Response Option Matrix (NROM)	1, 2, 4	Physical
DHS/USCG	* Activities Under the Combating Maritime Terrorism Strategic and Performance Plan, Maritime Security and Response Operations (Operation Neptune Shield (ONS))	1, 2, 4	Physical
DHS/USCG	Advanced Interdiction/Counterterrorism (AI/CT)	1, 2	Physical, Human
DHS/USCG	Area Maritime Security Training and Exercise Program (AMSTEP)	1, 2, 4	Physical, Human
DHS/USCG	Common Assessment and Reporting Tool (CART)	1, 2, 4	Physical
DHS/USCG	Military Outload (MOL) Security Support	1	Physical
DHS/USCG	Waterborne, Shoreside, and Aerial Patrols	1	Physical
DHS/USCG	Control Port Access Activity and Movement	1, 2	Physical, Human
DHS/USCG	Deployable Operations Group (DOG), including the Capabilities of the Tactical Law Enforcement Teams, Port Security Units, National Strike Force, Maritime Security Response Teams, and Maritime Safety and Security Teams (listed below)	1, 2, 4	Physical, Human
DHS/USCG	Escort Vessels	1	Physical

Department/Agency	MTS Program/Initiative * Denotes Key RMA	Maritime Goal Supported	Element (Physical, Cyber, Human)
DHS/USCG	Investigate Anomalies	1, 2	Physical
DHS/USCG	Maritime Force Protection Units (MFPUs), Transit Protection System (TPS)	1, 2	Physical
DHS/USCG DOJ/FBI	Maritime Operational Threat Response (MOTR) Plan	1, 2, 4	Physical, Human
DHS/USCG	Maritime Safety and Security Team(s) (MSST)	1, 2, 4	Physical, Human
DHS/USCG	Respond to and Recover from Terrorist Attack	1, 2, 4	Physical, Cyber
DHS/USCG	Specialized Use of Force	1	Physical
DOJ/FBI	Critical Incident Response Group (CIRG)	1	Physical, Cyber

Maritime Domain Awareness

Department/Agency	MTS Program/Initiative * Denotes Key RMA	Maritime Goal Supported	Element (Physical, Cyber, Human)
DHS/CBP	* Automated Targeting System	1, 2	Physical, Human
DHS/CBP	* Container Security Initiative (CSI)	1, 3, 4	Physical
DHS/CBP/USCG	Integrated Border Enforcement Team	1, 4	Physical, Human
DHS/CBP	Radiation Portal Monitors (RPMs)	1	Physical
DHS/CBP	Secure Freight Initiative (SFI)	1	Physical
DHS/USCG	Advanced Notice of Arrival	1, 4	Physical, Human
DHS/USCG	COASTWATCH	1, 4	Physical, Human
DHS/USCG	Collect, Monitor, Fuse, Analyze, Maintain, and Disseminate Information, Data, and Intelligence on Vessels, People, Cargo, Organizations, and Areas of Interest (including infrastructure) in the Global Maritime Environment	1, 2, 4	Physical, Human
DHS/USCG	Homeport	1, 2, 4	Cyber
DHS/USCG	Intelligence Contribution	1, 2, 4	Physical, Cyber, Human
DHS/USCG	Interagency Operations Centers (IOCs)	1, 2, 3, 4	Physical, Cyber, Human

Department/Agency	MTS Program/Initiative * Denotes Key RMA	Maritime Goal Supported	Element (Physical, Cyber, Human)
DHS/USCG	Long Range Identification and Tracking (LRIT)	1, 2, 4	Physical
DHS/USCG	Maritime Radiation Detection Programs	1	Physical
DHS/USCG	* Maritime Security Risk Analysis Model (MSRAM)	1, 2, 3, 4	Physical
DHS/USCG	* National Automatic Identification System (NAIS)	1, 4	Physical
DHS/DoT/DoD/ODNI	National Maritime Domain Awareness Coordination Office (NMCO)	1, 2, 4	Physical, Cyber
DHS/DoT/DoD/ODNI/Interagency Partners	National Maritime Stakeholders Board	1,2,4	Human
DHS/USCG/Aux	America's Waterway Watch (AWW)	1, 2, 4	Physical, Human
DHS/USCG	Underwater Port Security System (UPSS)	1, 2	Physical, Human
DHS/USCG	Update to HSIN-CS	1, 2, 4	Cyber
DOJ/FBI	FBI Field Intelligence Groups	1, 2, 4	Physical, Cyber, Human

Create and Oversee an Effective Maritime Security Regime⁴⁸

Department/Agency	MTS Program/Initiative * Denotes Key RMA	Maritime Goal Supported	Element (Physical, Cyber, Human)
DHS/CBP	Customs-Trade Partnership Against Terrorism (C-TPAT)	1, 4	Physical, Human
DHS/CBP/TSA/USCG/DNDO	DHS Small Vessel Security Strategy (SVSS) and Small Vessel Security (SVS) Implementation Plan	1, 2, 4	Physical
DHS/DNDO	Maritime Program Assistance	1	Physical
DHS/TSA/USCG/Industry	* Transportation Worker Identification Card (TWIC)	1, 2	Human
DHS/USCG	Conduct Security, Random and Suspect Vessel Boarding	1	Physical, Human
DHS/USCG	Information Sharing Environment (ISE) Suspicious Activity Reporting (SAR) Working Group	4	Human

⁴⁸ Programs, initiatives, and activities that contribute to implementation of regimes.

Department/Agency	MTS Program/Initiative * Denotes Key RMA	Maritime Goal Supported	Element (Physical, Cyber, Human)
DHS/USCG	* International Engagement/Enforce Foreign Flag Vessel Compliance with International Ship and Port Facility Security (ISPS) Code, Implement and Monitor Port State Control Measures	1, 2	Physical
DHS/USCG	International Engagement/Execute and Monitor the Special Interest Vessel (SIV) Program	1	Physical
DHS/USCG	* International Engagement/International Port Security Program	1	Physical
DHS/USCG	Lead Area Maritime Security Committees (AMSCs)	1, 2, 4	Physical, Human
DHS/USCG	* MTSA/Review, Approve, and Enforce Compliance with Plans and Regulations for Domestic Vessel, Facility, and Outer Continental Shelf (OCS) Facility Security Plans, Area Maritime Security Plans (AMSPs), Vessel Compliance	1, 2	Physical, Human
DHS/USCG	Underwater Terrorism Preparedness Plans (UTPPs)	1	Physical, Human
DOJ/FBI/Multiple Agencies	Joint Terrorism Task Forces (JTTFs)	1, 3, 4	Physical, Cyber, Human
DOJ/FBI	Maritime Liaison Agent Program (MLAP)	1, 2, 4	Physical, Human
DOT/MARAD/USCG	Maritime Administration Port Readiness Program	1	Physical
DOT/MARAD	MTSA Section 109, Training and Certification of Maritime Security Personnel	1	Human

3.6 Metrics/Measurement Process

Four key attributes of successful performance measures (also called metrics) are identified by experts and leading organizations,⁴⁹ and cited by the Government Accountability Office (2009). Specifically, measures should be (1) quantifiable, (2) meaningful, (3) repeatable and consistent, and (4) actionable. Performance measures can be used to facilitate decisionmaking and improve performance and accountability through the collection, analysis, and reporting of relevant data. The purpose of measuring performance is to monitor the status of measured activities and facilitate improvement in those activities by applying corrective action based on the observed measurements. Such measurements can be used to monitor the accomplishment of goals and objectives, and analyze the adequacy of control activities. Thus, performance measures should provide managers and other stakeholders with timely, action-oriented information in a format that facilitates decisions aimed at improving program performance.⁵⁰

⁴⁹ Leading organizations are prominent, nationally known organizations, academic institutions, and State agencies. With regard to Report No. GAO-09-617, the focus is on comprehensive enterprise-wide information security programs. It is assumed, however, that the four key attributes of successful measures are transferable; this is supported on page 9 of the report where the findings conformed to prior reports on effective performance measurement and reporting practices in Report No. GAO-05-927.

⁵⁰ Report No. GAO-09-617, p. 3.

The maritime transportation mode's sector-specific program measurement scheme will leverage existing information-sharing mechanisms and partner to measure progress toward national objectives to enhance the security of and protection of U.S. interests in the maritime domain. One particular agency or department does not own all programs, activities, and initiatives, and management can extend to a vast number of stakeholders in the public and private sectors. The complexity of the maritime mode and the Transportation Systems Sector demands a high degree of alignment and coordination of protective programs, activities, and tools. This complexity also demands that MTS partners are considered in the broadest context (e.g., government, private, and international sectors). Through the NIPP risk management framework, program and activity measurements from various program leads are reported vis-à-vis the SSA and are captured in the Transportation Systems Sector CIKR Protection Annual Report, an annex to the National CIKR Protection Annual Report.

The SSA will continue to work with its public and private sector partners to develop, refine, and report on risk reduction metrics, taking into consideration the key attributes of successful performance measures that support national-level objectives. Risk mitigation activities, for which programs and activities cascade, are presently categorized into the following groups: (1) Risk Reduction Tools and Methods, (2) Maritime Security and Response Operations, (3) Maritime Domain Awareness, and (4) Effective Maritime Security Regime/Information Sharing. Information-sharing programs and activities cascade across all four groups.

Key attributes, as applied to the MTS and the maritime mode, are as follows:

- **Quantifiable.** The aim of metrics is quantifiable value; qualitative measures may also be used, including in national-level reporting. Quantitative data may not always be included in annual reports because when certain data is combined with other information, the output may fall into the category of Sensitive Security Information, which is a designation given to particular information in the Transportation Systems Sector. This does not mean that the quantifiable data is not being collected, analyzed, and used to inform decisions through other venues.
- **Meaningful.** Meaningful measures have targets or thresholds for each measure to track progress over time, are defined with clarity to precisely reflect what is being measured, and are linked to national or organizational priorities. Priorities, for example, might include quality, timeliness, or the best use of available resources.
- **Repeatable and Consistent.** Measures should be repeatable and able to produce consistent results by ensuring they are defensible, auditable, and use readily obtainable data. A measurement process implemented consistently over time to ensure that measurements are comparable with each other is optimal.
- **Actionable.** Measures that are actionable support the decisionmaking process and drive the behavior of those who are responsible for the control activities reflected in the measures.

Adherence to key practices, as identified by leading organizations and experts, also includes focusing on risks, involving stakeholders, assigning accountability, and linking to business goals.⁵¹ With respect to critical infrastructure, the NIPP risk management framework includes measuring effectiveness that feeds into a feedback loop. NIPP specific outcome metrics and descriptive data are reported in two ways—through the National Coordinator Progress Indicators and through the Sector Progress Indicators. Collectively, these metrics and data will provide a holistic picture of the health and effectiveness of the national and sector CIKR efforts. Progress toward modal goals will also be informed largely by existing Office of Management and Budget program efficiency measures.

Title 46 U.S.C. 70306 directs the Secretary of Homeland Security to report annually “on the threat of terrorism to U.S. ports and vessels operating from those ports ... [and to] include a description of those activities undertaken under Title I of MTSA and an analysis of the effect of those activities on port security against acts of terrorism.”

⁵¹ Report No. GAO-09-617.

The USCG continues to apply a risk-based methodology to ascertain the effectiveness of terrorism risk reduction measures. To ascertain risk reduction estimates, the USCG uses a risk-based analysis to measure the performance of its PWCS mission. The process combines national threat and field-level vulnerability and consequence data captured through MSRAM. A yearly percentage reduction is captured using an annual baseline.⁵²

⁵² Threat of Terrorism to U.S. Ports and Vessels, DHS Annual Report to Congress, 2009.

4. Security Gaps

Effective practices for identifying and mitigating security gaps are contained in this section. The MTS is a regulated environment; government and industry build efficiency into the system with effective practices. The following describes some of the effective practices in the MTS, to include security guidelines, security requirements, compliance process, training and exercises, and grant programs; these practices and their output help to identify, prioritize, and mitigate security gaps.

4.1 Security Guidelines

Security guidelines are initiatives and activities implemented on a voluntary basis to enhance the security of the MTS. They are present at the various stratifications of partnership levels, from the international to the local and tribal levels, and across the public, private, and nonprofit sectors. The following represents a sample of these guidelines:

- **The Container Security Initiative (CSI).** CSI is a series of bilateral, reciprocal agreements that, among other matters, position U.S. Customs and Border Protection (CBP) personnel at selected foreign ports to pre-screen U.S.-bound containers. CSI is operational in 58 seaports, in 32 countries worldwide. More than 80 percent of the maritime containerized cargo destined for the U.S. originates or passes through a CSI port, affording the U.S. Government the opportunity to identify and examine the highest risk containers. In 2009, more than 56,000 overseas examinations were performed.⁵³
- **The Customs-Trade Partnership Against Terrorism (C-TPAT).** Under CBP's layered, defense-in-depth strategy against terrorism, C-TPAT is the CBP initiative that partners, on a voluntary basis, with members of the trade community. CBP and members of the trade community collaborate to better secure the international supply chain to the United States in support of homeland security by ensuring the integrity of private sector security practices, and communicating and verifying the security guidelines of business partners within the supply chain. In support of this initiative, CBP assigns a C-TPAT Supply Chain Security Specialist who works with a private company to validate and enhance security throughout the company's supply chain. C-TPAT is one of CBP's initiatives that helps the agency to achieve its twin goals—the security and facilitation of trade moving into the United States.
- **International Port Security Program (IPSP).** The USCG, through its IPSP, encourages bilateral or multilateral discussions with nations around the world in an effort to exchange information and share best practices that align the implementation and enforcement requirements of the MTSA with the ISPS Code and other international maritime security standards. A component of the program includes reciprocal country port security visits and the sharing of best practices. These practices are published via Homeport and are discussed in bilateral and multilateral forums. Special emphasis is placed on sharing cost-effective security practices and innovative applications that have a significant impact on facility security.

⁵³ Ibid.

- **America's Waterway Watch (AWW).** AWW is an outreach program for enhancing the awareness and participation of those who live, work, or play around America's waterfront areas. Its aim is to generate more information and reports of suspicious activities. It is carried out by Active, Reserve, and Auxiliary personnel of the USCG. USCG reserve personnel concentrate on connecting with businesses and government agencies, while auxiliary personnel focus on building AWW awareness among the recreational boating public.
- **Sector Partnership Model.** The Sector Partnership Model brings together private sector CIKR owners and operators, or their representative trade or equivalent associations, to coordinate CIKR efforts and activities. These efforts and activities may include planning, development, and implementation of CIKR protection and preparedness programs; operational activities related to CIKR protection and resilience, including incident response and recovery; and development and support of national policies and plans.
- **State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC).** Formed in 2007, the SLTTGCC strengthens the sector partnership framework by fully integrating State, local, tribal, and territorial governments into the CIKR protection process. Members are geographically diverse and offer knowledge from a wide range of professional disciplines; representatives from the SLTTGCC efforts have shown success in information-sharing efforts to gain regional perspectives. The SLTTGCC also coordinates and has a standing member on the Regional Consortium Coordinating Council (RCCC), which was formed in 2008 with the primary mission of injecting regional perspectives into the deliberative processes of numerous Federal agencies and government and sector working groups.
- **The USCG Deployable Operations Group (DOG).** The DOG was formed in 2007 and provides properly equipped, trained, and organized deployable specialized forces (DSFs) units to rapidly provide the USCG, DHS, DoD, DOJ, and other interagency operational commanders with adaptive force packages. DSF units in the DOG structure include Maritime Safety and Security Teams, the Maritime Security Response Team, Tactical Law Enforcement Teams, Port Security Units, the National Strike Force, the National Strike Force Coordination Center, and USCG personnel assigned to the Navy's Naval Coastal Warfare squadrons. Interoperability is enhanced through national interagency exercises and planning conferences.

4.2 Security Requirements

Security requirements are regulatory in nature. The Federal maritime security regime creates a comprehensive framework to enhance the security of the MTS by preventing a TSI. Some key requirements of 33 CFR, which are in place, include:

- A three-tiered maritime security regime (9,200 Domestic Vessel Security Plans; 3,200 Facility Security Plans; 43 AMSPs; and the NMTSP).
- Security Advisory Committees; the National Maritime Security Advisory Committee; and 43AMSCs.
- MARSEC levels. Along with the security activities performed by vessel and facility owners and operators, the USCG conducts routine maritime security operational activities; both activities are complementary and are implemented within the MARSEC levels.
- Notice of Arrival (NOA). At least 96 hours in advance, vessels destined for a U.S. port or place must provide a NOA, unless they fall under the 24/12-hour exceptions (33 CFR 160).
- CBP regulations require the advance and accurate presentation of cargo declaration information before loading cargo onto a vessel at the foreign port (the 24-hour rule). Specifically, customs regulation 19 CFR 4.7 was amended to provide that, pursuant to 19 U.S.C. 1431(d), for any vessel subject to entry under 19 U.S.C. 1434, upon its arrival in the United States, CBP must receive the vessel's cargo declaration from the carrier 24 hours prior to loading the cargo at the foreign port.
- The Security and Accountability for Every Port Act of 2006 (SAFE Port Act, Public Law 109-347) is a comprehensive maritime and cargo security bill. The bill, as implemented, strengthens port security across the Nation by establishing improved cargo

screening standards, providing incentives for importers to enhance security measures, and implementing a framework to ensure the successful resumption of shipping in the event of a terrorist attack, while preserving the flow of commerce.

4.3 Assessment and Compliance Process

Government agencies assess compliance with maritime regulations through two main processes: (1) the review and approval of regulatory requirements, and (2) compliance assessment.

The review and approval of regulatory requirements is backed by on-site inspections and spot checks. The USCG published minimum required contents for MTSA-required vessel and facility security plans. These plans are reviewed and approved by the USCG; compliance with these requirements is assessed during on-site inspections. The review and approval of local port-level AMSPs also fall under this main process category.

Compliance assessment is the concept of layered defense. No single security program is a stand-alone program; each is part of a layered security regime.

4.4 Training and Exercises

Training is an integral part of implementing protective programs and is conducted regularly by owners and operators. Exercises provide an opportunity to identify gaps in existing implementation plans while improving familiarity with the contents and competence in execution. Although there are some regulatory requirements for training and exercises, other voluntary training and exercise venues offer additional opportunities for collaboration. Scenario-based training can offer a systems perspective in the protection of critical infrastructure; participation in training and exercises occurs at the national to the local levels. MTS stakeholders must seek committee input at the national, State, regional, and local training and exercise annual and five-year planning sessions.

The DHS Office of Infrastructure Protection has promoted various training opportunities for CIKR partners. This training is provided through Webinars, and via online platforms. The development of outreach and training programs for CIKR partners continues to advance in the area of CIKR.

4.5 Grant Programs

As a component of the Infrastructure Protection Program (IPP), the Port Security Grants Program (PSGP) seeks to assist the Nation's ports in obtaining the resources and capabilities required to support the National Preparedness Goals and National Priorities. The National Critical Infrastructure Prioritization Program informs grant program and award selection. Recent criteria for the grants focus on the ability to create a sustainable, risk-based effort to protect critical port infrastructure from terrorism, particularly attacks using explosives and non-conventional threats that could cause a major disruption to commerce. PSGP funds are intended to assist ports in enhancing MDA and risk management capabilities to prevent, detect, respond to, and recover from attacks involving IEDs; chemical, biological, radiological, nuclear, and high-yield explosives (CBRNE); and other non-conventional weapons, as well as training and exercises and TWIC implementation.

4.6 Challenges for MTS Operations

There are many challenges that remain on a day-to-day basis for meeting national-level objectives and furthering the vision statement of the maritime transportation mode. Several of the programs, initiatives, and risk mitigation activities used to address MTS challenges have been described previously in this national-level plan. The following are near-term areas of emphasis:

- *Managing Risks to CIKR.* Cross-sector dependencies and interdependencies will remain a focus. The identification of risk within the supply chain, which could affect the MTS and vice versa, will continue to be assessed.
- *Small Vessel Security.* Determining the intent of small vessels operating in close proximity to CIKR remains a challenge in the U.S. and around the world; this challenge is addressed in the USCG Small Vessel Security Strategy and will continue to remain a priority.
- *Especially Hazardous Cargo (EHC) Security.* The identification and mitigation of risk associated with EHC, including during its transit through the intermodal supply chain, continues to be an important aspect of domain awareness and an area of focus.
- *Cyber Threat.* The Nation must be protected against cyber risk elements and be made more resilient through the application of a flexible and adaptable cyber incident response capability. The exploitation of cyberspace could place MTS critical systems, networks, and data at risk; identification and understanding of the cyber risk element is a priority.
- *Challenges of the Arctic System.* The changing physical conditions on our Arctic coast present a variety of challenges. This necessitates the development of a plan for responsible governance of the MTS to protect the environment and our economic and energy security interests. The Interagency Oceans Policy Task Force is developing a comprehensive national policy for the ocean, coasts, and Great Lakes, including marine spatial planning, and a strategy to best implement the policy.

5. The Way Forward

The MTS continues to evolve and respond to changes; however, the complexity of the environment remains. Cooperation, collaboration, and information sharing between and among security partners shall remain a priority. The goals and objectives of this plan, along with the requirements placed upon the SSA shall be implemented, as appropriate. Nothing in this plan alters, or impedes the ability of the authorities of Federal departments and agencies to perform their responsibilities under law. This plan is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable by law or in equity, against the U.S., its departments or agencies, or other entities, its officers or employees, or any other person.

Maritime Enterprise Mapping: Directives and Guidance

Maritime Enterprise Mapping: Directives and Guidance document is in place to guide future direction and the way forward, including program development, management, and implementation. This map shall continue to evolve as a living document. A baseline map is appendix E.

The National Strategy for Maritime Security outlines three broad principles: (1) preserve the freedom of the seas; (2) facilitate and defend commerce to ensure the uninterrupted flow of shipping; and (3) facilitate the movement of desirable goods and people across our borders, while screening out dangerous people and material. These are the guiding principles and deep-seated values enshrined in the U.S. Constitution and reflected in applicable domestic and international law addressing maritime security activities.⁵⁴

⁵⁴ National Strategy for Maritime Security, Section III, pp. 7–8, 2005.



Appendix A: Related Plans and Strategies

Plans

Area Maritime Security Plans

Maritime Infrastructure Recovery Plan, 2006

Maritime Operational Threat Response Plan, 2006

Maritime Security Plans

National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency, 2009

Outer Continental Shelf Facility Security Plans

Plan to Re-Establish Cargo Flow After a TSI (Appendix C), 2005 (SSI)

Underwater Terrorism Preparedness Plans

USCG Combating Maritime Terrorism Strategic and Performance Plan, 2008

Vessel and Facility Security Plans

Strategies

DHS Small Vessel Security Strategy, 2008

National Response Framework, 2008

National Security Strategy, 2006

National Strategy for Combating Terrorism, 2006

National Strategy for Homeland Security, 2007

National Strategy for the Marine Transportation System: A Framework for Action, 2008

The National Strategy for Maritime Security, 2005

National Strategy for the Physical Protection of Critical Infrastructure and Key Assets, 2003

The National Strategy to Secure Cyberspace, 2003

National Strategy for Transportation Security (now incorporated into TS SSP 2010), 2005

One Team, One Mission, Securing Our Homeland: U.S. Department of Homeland Security Strategic Plan, 2008

Recovering from Disasters: The National Transportation Recovery Strategy, 2009

Strategy to Enhance International Supply Chain Security, 2007

USCG Combating Maritime Terrorism Strategic and Performance Plan, 2008

USCG Strategy for Maritime Safety, Security, and Stewardship, 2007

Annex C: Mass Transit and Passenger Rail



Contents

1. Executive Summary	211
2. Overview of the Mode	215
2.1. Background	215
2.2. Vision for the Mode	216
2.3. Description of the Mode	216
2.3.1. Overview	216
2.3.2. Responsibilities	217
2.3.3. Security Risk	220
3. Implementation Plan	223
3.1. Strategies and Objectives	223
3.1.1. Expanding Partnerships for Security Enhancement	223
3.1.2. Continuously Advancing the Security Baseline	224
3.1.3. Building Security Force Multipliers	225
3.1.4. Providing Security Information Leadership	225
3.1.5. Deploying Tools to Mitigate High Consequence Risks	226
3.2. Strategic Risk	228
3.3. Tactical/Operational Risk	228
3.4. Security Programs and Processes	229
3.4.1. Surface Transportation Security Inspection Program	229
3.4.2. VIPR Teams	230
3.4.3. Information-Sharing	231
3.4.4. Security Training and Awareness	231
3.4.5. National Tunnel Security Initiative	232
3.4.6. Security Technology Deployment	232
3.4.7. Technology Research and Development	233
3.4.8. International Initiatives	233
3.4.9. Grant Programs	233
3.5. Effective Practices, Security Guidelines, and Security Standards	234
3.5.1. Security Guidelines	234
3.5.2. Security Standards Development	234
3.5.3. Rulemaking	235

4. Metrics	237
5. Security Gaps and Mitigation Strategies	239
5.1 Information Sharing	239
5.2 Employee Security Training	239
5.3 Security Awareness Campaigns	240
5.4 Research and Development and Technology Deployment	240
5.5 Underwater/Underground Tunnels	241
5.6 Drills and Exercises	241
5.7 Cybersecurity	242
6. Way Forward	243

List of Figures

Figure C3-1: Process Model	223
Figure C4-1: Objectively Measured Risk Reduction	238

List of Tables

Table C3-1: Mass Transit Objectives	227
-------------------------------------	-----

1. Executive Summary

This updated plan for mass transit and passenger rail security addresses the objectives and priorities described in the 2010 Transportation Systems Sector-Specific Plan (SSP). It also incorporates the requirements of the National Strategy for Public Transportation Security enumerated in Title XIV of the Implementing Recommendations of the 9/11 Commission Act of 2007¹ and updates the mass transit plan included in the National Strategy for Transportation Security, as required by the Intelligence Reform and Terrorism Prevention Act of 2004, as amended.²

Since the initial publication of this plan in 2007, the Transportation Security Administration (TSA), working with its public and private sector partners, has implemented a variety of programs and initiatives that have enhanced security in mass transit and passenger rail systems. While a great deal has been achieved, the public transportation industry and its partners continue to face many challenges in their efforts to provide a secure and protected travel environment. The mass transit and passenger rail systems are open, serving millions of passengers every day. The networks cover wide geographical areas providing numerous points of access and connections to other means of transportation, leading to high passenger turnover, which is difficult to monitor effectively. As the public and private partners continue their efforts to implement plans to secure the mass transit and passenger rail systems, new challenges arise. In this context, government and industry continue to work closely and collectively to provide a secure environment for passengers and employees through training, public outreach, exercises, hardening of physical assets, and expanding visible/covert, random, and unpredictable security measures.

Priorities are reached and objectives achieved by applying risk management principles set forth in the SSP. These principles ensure that risk reduction and protection measures are implemented in mass transit and passenger rail systems where they offer the most benefit both in response to specific threats and in the general threat environment. In this context, the mass transit and passenger rail security strategy is guided by five key principles.

Expand Partnerships for Security Enhancement: Proactive and continuous collaboration with senior executives, law enforcement chiefs, and security managers for mass transit and passenger rail agencies; State, tribal, and local government officials, law enforcement, and emergency responders; and Federal partners to foster regional security coordination and to integrate the spectrum of available resources for enhanced deterrence and response capabilities. Engagement occurs directly with these key officials and through such collaborative forums as the Mass Transit Sector Coordinating Council (SCC), the Transit Policing and Security Peer Advisory Group, the Regional Transit Security Working Groups in higher risk areas, and the annual Transit Safety and Security Roundtables. The Transit Safety and Security Roundtables bring together the law enforcement chiefs and security directors of the largest 50 to 100 mass transit and passenger rail agencies with their Federal security partners to discuss specific terrorism prevention and response challenges and collaborate in advancing effective solutions. The overall effort aims to ensure

¹ Public Law 110-53, August 3, 2007.

² Public Law 108-458, December 17, 2004.

coordinated development and implementation of effective security strategies nationally and to build collaborative regional networks that expand capabilities to prevent acts of terrorism and to respond to and recover from threats and security incidents.

Elevate the Security Baseline: Accomplishment of thorough security and risk assessments on mass transit and passenger rail systems nationally, with particular emphasis on the 100 largest in passenger volume (the 100 largest systems collectively account for more than 80 percent of all users of public transportation). The assessment results are used to establish a security profile and baseline posture for transit or passenger rail security programs; track improvement or diminution from the baseline; and determine program decisions and future needs.

- Through the Transportation Systems Sector Risk Assessment (TSSRA), TSA has evaluated threat, vulnerability, and consequence in a wide range of terrorist attack scenarios for each mode of transportation. For mass transit and passenger rail, this assessment considered more than 200 scenarios, rating threat capabilities and likelihood of execution; vulnerabilities of rail and bus systems and infrastructure; and potential consequences in casualties, property damage, and impacts on the transportation network. The resulting risk ranking enables setting of informed mitigation priorities, both across the sector and by individual mode, for collaborative security strategies, program development and resource allocations.
- Under the Baseline Assessment for Security Enhancement (BASE) program, TSA Transportation Security Inspectors-Surface (TSIs), assess the security posture of mass transit and passenger rail agencies in 17 Security and Emergency Management Action Items. The Action Items were developed in a joint effort with TSA, the Federal Transit Administration (FTA), and mass transit and passenger rail operating and security officials engaged through the Mass Transit SCC, and cover a range of areas that are foundational to an effective security program. The specific purpose is to evaluate, across multiple areas with a thorough checklist and narrative responses, the effectiveness of security programs, procedures, and measures developed and implemented by mass transit and passenger rail agencies. The results of these assessments inform development of risk mitigation priorities, security enhancement programs, and resource allocations, notably transit security grants. The assessments also provide the critical underpinning of the security strategy continuous improvement process. Conducted on a periodically recurring basis, the BASE assessments enable comparative analysis of results to provide an objective evaluation of progress in mitigating security risk, both by individual system and nationally.
- Finally, TSA is developing and fielding a risk assessment capability focused on individual mass transit and passenger rail agencies, their regional security partners, and connecting and adjoining transportation systems. This effort aims to produce several risk and vulnerability assessment tools integrated in a single platform to enable TSA and its security partners in the Department of Homeland Security (DHS) to conduct joint assessments of mass transit and passenger rail agencies, employing resources more efficiently and mitigating audit fatigue.

Build Security Force Multipliers: A persistent effort aims to expand informed, capable “eyes and ears” for security through targeted awards under the Transit Security Grant Program (TSGP) for employee security training, anti-terrorism exercises, public awareness campaigns, and fielding specially-trained and equipped anti-terrorism law enforcement teams and technological systems to enhance detection and deterrence capabilities. The total risk-based TSGP investment in mass transit and passenger rail security for the period of fiscal year (FY) 2006 through FY 2009, including the supplement under the American Recovery and Reinvestment Act of 2009, is approximately \$1.5 billion. Supporting TSA programs include the Intermodal Security Training and Exercise Program (I-STEP), which integrates mass transit and passenger rail agencies with regional law enforcement and emergency response partners. I-STEP expands and enhances coordinated deterrent and incident management capabilities. The “Bomb Squad Response to Transportation Systems-Mass Transit” initiative features scenario-based exercises which place bomb technicians from law enforcement in the mass transit and passenger rail environment and expands regional capabilities to respond to threats or incidents involving suspected explosive devices.

Lead Information Assurance: Joint briefings of classified intelligence by the DHS Office of Intelligence and Analysis, TSA Office of Intelligence (TSA-OI), and the Federal Bureau of Investigation (FBI) are simultaneously presented to mass transit and passenger rail security directors and law enforcement chiefs in 16 metropolitan areas via the Joint Terrorism Task Force (JTTF).

secure video-teleconferencing system. In addition, TSA has deployed secure communications equipment to Amtrak and to the top-ranked agencies based on passenger volume. Secure cell phones maintained by TSIs provide regional capabilities for rapid communication of classified information. Also, the periodic dissemination of TSA Mass Transit Security Awareness Messages provides relevant and usable intelligence products with a practical security context to mass transit and passenger rail operators. TSA OI's Transportation Security-Information Sharing and Analysis Center (TS-ISAC) offers a website where unclassified intelligence products can be housed and discussions with stakeholders regarding intelligence issues can take place. This site is located on the Homeland Security Information Network (HSIN) and is directly linked to the Homeland Security Information Network-Critical Sectors (HSIN-CS) and individual modal sites. The recently established partnership with the Public Transit Information Sharing and Analysis Center (PT-ISAC) and the American Public Transportation Association (APTA) provides access to similar materials gathered by TSA to support mass transit and passenger rail officials. In a collaborative effort, the TSA Mass Transit and Passenger Rail Security Division (the Division) and OI, FTA, the PT-ISAC, and representatives of the mass transit and passenger rail agencies are developing recommendations on specific actions to enhance the scope, accuracy, timeliness, and efficiency of information sharing. A primary objective of this effort is producing a unified, comprehensive intelligence and security information-sharing platform for the mode, with reports and other materials on security technologies as an essential component.

Protect High Risk Assets and Systems: The strategic priority of active deterrence is advanced through coordinated, joint security operations and random security inspections, supported through TSGP awards that focus on expanding operational capabilities in mass transit and passenger rail systems. Several mass transit and passenger rail agencies have implemented or approved programs for random inspections of passengers' bags. TSA supports implementation of random, unpredictable security activities designed to create changing layers of security through multiple means.

- Visible Intermodal Prevention and Response (VIPR) team deployments augment security capabilities for random patrols and surges, behavior detection, and explosives detection through canine teams and explosives security specialization. More than 900 VIPR operations were conducted in mass transit and passenger rail systems since 2005. A growing number of agencies are partnering with TSA to deploy VIPR teams on a recurring, random, and unpredictable basis, integrating this capability into their security programs.
- Risk-based deployment of TSA-certified explosives detection canine teams expand systems' deterrence and detection capabilities, with 82 teams deployed among 15 systems as of December 2009. This program will continue to offer mass transit and passenger rail agencies the means to secure and employ a flexible security enhancement resource. Jointly planned and executed security surges integrate mass transit and passenger rail agencies with Federal, State, and local law enforcement and security partners in a unified effort to prevent acts of terrorism through collaborative random security activities. The most extensive demonstration of this effort has occurred in the Northeast Corridor with the largest coordinated rail security operations in the United States. Unified law enforcement officers from nearly 150 departments supporting more than 150 passenger rail stations from Fredericksburg, VA, to Portland, ME, were simultaneously and operationally engaged during same day morning and evening rush hours. Similar deterrence operations are being conducted in metropolitan areas across the country with mass transit and passenger rail agencies and local law enforcement departments simultaneously collaborating in random patrols and surges.
- Coordinated technology development and testing in partnership with the DHS Science and Technology Directorate is ongoing. The efforts focus on enhancing capabilities, through flexible application of mobile and fixed technologies to protect high risk assets and systems, such as underwater tunnels and high volume terminals and stations. Technologies are being developed and evaluated to detect and deter terrorist activity and prevent attacks in the demanding transit environment. TSA works continuously to expand opportunities to employ its resources and capabilities to elevate the deterrent posture in mass transit and passenger rail.



2. Overview of the Mode

2.1 Background

In 2007, TSA and the United States Coast Guard led the effort to develop and implement the Transportation Systems SSP and its modal annexes, including the Mass Transit Annex. The SSP, issued in June 2007, was one of the original 17 sector plans required by the National Infrastructure Protection Plan (NIPP), which implement the requirements of Homeland Security Presidential Directive 7 (HSPD-7): Critical Infrastructure Identification, Prioritization, and Protection (December 13, 2003). The Mass Transit and Passenger Rail Annex to the SSP was developed in collaboration with DOT, FTA, and in close cooperation with other Federal, State, local, and industry partners. The annex provided a blueprint for enhancing the security of mass transit and passenger rail assets, systems, and networks that provide services essential for the Nation's security and economic vitality. This document serves as the 2010 update to the Mass Transit and Passenger Rail Annex. It also serves as the update for the mass transit plan of the National Strategy for Transportation Security required by the Intelligence Reform and Terrorism Prevention Act of 2004, as amended. This annex further serves as the National Strategy for Public Transportation Security mandated by the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act). Enactment of this statute followed the issuance of the Transportation Systems SSP and its modal annexes. Section 1404 of the 9/11 Act requires the Secretary of Homeland Security to develop and implement a modal plan for public transportation security, entitled the "National Strategy for Public Transportation Security." Pursuant to this section, the purpose of the plan is to establish guidelines for public transportation entities that minimize security threats and maximize the ability of public transportation systems to mitigate damage resulting from terrorist attack or other major incident. In developing the National Strategy for Transportation Security, Section 1404 of the 9/11 Act further requires the Secretary to:

- Use existing security assessments;
- Consult all relevant security partners, including public transportation agencies, nonprofit labor organizations representing public transportation employees, emergency responders, public safety officials, and other relevant partners;
- Describe prioritized goals, objectives, policies, actions, and schedules to improve the security of public transportation;
- Include a description of the roles, responsibilities, and authorities of Federal, State, and local agencies, tribal governments, and appropriate security partners;
- Identify and address gaps and redundancies; and
- Provide a process for coordinating existing or future security strategies and plans for public transportation, including the NIPP; Executive Order No. 13416: Strengthening Surface Transportation Security dated December 5, 2006; the memorandum of understanding between DHS and DOT on Roles and Responsibilities dated September 28, 2004; and subsequent annexes and agreements.

Combining the various mandated plans into a single, comprehensive strategic plan is consistent with the direction of Sections 1404 and 1511 of the 9/11 Act requirement to use relevant existing assessments and strategies developed by DHS or other Federal agencies and to provide a process for coordinating existing or future strategies and plans for public transportation including the NIPP, Executive Order No. 13415, and other memoranda of understanding and agreements.

2.2 Vision for the Mode

The vision for the mass transit and passenger rail mode is a secure, resilient public transportation system. This will be achieved by employing a unified security approach integrating mass transit and passenger rail agencies with Federal, State, local, territorial, and tribal law enforcement and security partners in varied, random, and unpredictable operational activities, supported by infrastructure hardening, security technologies, well-trained employees, and a vigilant public to assure the efficient flow of passengers and encourage expanded use of the Nation's transit and rail services.

2.3 Description of the Mode

2.3.1 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, 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. The mass transit and passenger rail mode does not include over-the-road motorcoach operators, school bus systems, or 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 type 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.³ There are 565 transit systems that operate in urban areas with a population greater than 50,000 persons. Amtrak operates the Nation's primary intercity passenger rail service over a 22,000-mile network, primarily over leased freight railroad tracks, serving more than 500 stations in 46 states and the District of Columbia. In fiscal year (FY) 2008, 28.7 million passengers traveled in the Amtrak system. About two-thirds of this ridership is concentrated in the "Northeast Corridor," between Boston and Washington, D.C. Additionally, Amtrak operates commuter rail services in certain jurisdictions on behalf of State and regional transportation authorities. Since 1995, the transit and commuter ridership in the United States has grown by 38 percent and this growth will likely continue in light of the volatility of fuel prices and increasing road congestion. In 2008, Americans took 10.7 billion trips using mass transit and passenger rail. APTA estimates that about 35 million trips are taken each weekday in the United States. 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.

The mass transit and passenger rail mode includes thousands of employees, operational and maintenance facilities, construction sites, utilities, administrative facilities, and thousands of computerized networks, which facilitate operations and ensure efficient and reliable service.

³ FTA National Transit Database (NTD), <http://www.ntdprogram.com/ntdprogram/>.

- Heavy rail systems—subway systems like New York City’s transit system and Washington, DC’s Metrorail—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 operate 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 during morning and evening peak periods).
- Light rail systems are typically characterized by lighter weight passenger rail cars, drawing electric power from overhead power lines, and often operating in shared-use rights-of-way, including streets with vehicular traffic.
- Bus transit systems provide frequent transportation service for the primary purpose of moving passengers between bus stops, often through multiple connections.
- Commuter bus systems provide passenger services, primarily during morning and evening peak periods, between an urban area and more distant outlying communities in a greater metropolitan area.

2.3.2 Responsibilities

Securing the Nation’s passenger rail and mass transit systems is a shared responsibility, depending upon coordinated action by Federal, State, tribal, and local governments; mass transit and passenger rail agencies and their employees; and the passengers who ride these systems. Since the attacks of September 11, 2001, the role of the Federal Government in this area continues to evolve. Previously, DOT—namely, FTA and the Federal Railroad Administration (FRA)—served as the primary Federal entity for mass transit and passenger rail security matters. In response to the attacks of September 11, 2001, Congress enacted the Aviation and Transportation Security Act (ATSA), which created TSA within DOT and provided TSA with broad responsibility and authority for security in all transportation modes. With the passage of the Homeland Security Act of 2002,⁴ TSA, and its statutory authorities and responsibilities, transferred to DHS, along with more than 20 other agencies.

In executing its responsibilities and functions, TSA is specifically empowered to develop policies, strategies, and plans for dealing with threats to transportation.⁵ As part of its security mission, 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.⁶ TSA also is to enforce security-related regulations and requirements,⁷ oversee the implementation and ensure the adequacy of security measures at transportation facilities,⁸ and carry out other appropriate duties relating to transportation security.⁹ Under its broad regulatory authority to achieve ATSA’s objectives, TSA 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.¹⁰ TSA is also charged with serving as the primary liaison for transportation security to the intelligence and law enforcement communities.¹¹

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

⁴ Public Law 107-296.

⁵ 49 U.S.C. 114(f)(3).

⁶ 49 U.S.C. 114(f)(1)-(5).

⁷ 49 U.S.C. 114(f)(7).

⁸ 49 U.S.C. 114(f)(11).

⁹ 49 U.S.C. 114(f)(15).

¹⁰ 49 U.S.C. 114(l).

¹¹ 49 U.S.C. 114(f)(15).

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.¹²

Pursuant to the 9/11 Act, TSA exercises a range of authorities specifically related to the mass transit and passenger rail security mission. These include:

- Management of the TSGP, in partnership with FEMA;¹³
- Deployment of TSA's TSIs "to assist surface transportation carriers, operators, owners, entities, and facilities to enhance their security program against terrorist attack and other security threats and to assist the Secretary in enforcing applicable surface transportation security regulations and directives";¹⁴
- Coordination and execution of a terrorism prevention exercise program;¹⁵ and
- Augmentation of security in mass transit and passenger rail systems, in coordination with the agencies' law enforcement and security officials and their local security partners, by deployment of VIPR teams.¹⁶

Additionally, in consultation with mass transit and passenger rail community stakeholders and other interested constituencies, work is ongoing to produce the regulations directed by the 9/11 Act on security training programs¹⁷ and security plans.¹⁸ These efforts are leveraging the insights and context gained from the comprehensive security assessments conducted under the BASE program as well as the progress attained through initiatives focused on these areas under the TSGP.

DOT retains some security-related responsibilities. FTA conducts a range of safety and security activities, including employee 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 at least one percent, and may spend more, of their annual allocations on security-related projects, or certify that they do not need to do so (based on criteria such as the availability of non-5307 funds for funding security needs or a record of assessments indicating no deficiencies). For transit agencies in areas over 200,000 in population, only security-related capital projects are eligible to meet the one 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 one percent threshold. Additionally, under the Safe, Affordable, Flexible, Efficient Transportation Equity Act – A Legacy for Users (SAFETEA-LU),¹⁹ the definition of capital programs has been expanded to include security and emergency planning, training, and exercises, thus providing more flexibility to larger transit agencies in meeting the one percent threshold.

¹² 49 U.S.C. 114(f)(1) and (5).

¹³ See sections 1406 and 1513, 9/11 Act (Public Law 110-53).

¹⁴ See section 1304, 9/11 Act.

¹⁵ See sections 1407 and 1516, 9/11 Act.

¹⁶ See section 1303, 9/11 Act.

¹⁷ See sections 1408 and 1517, 9/11 Act.

¹⁸ See sections 1405 and 1512, 9/11 Act.

¹⁹ Public Law 109-59, August 10, 2005.

FTA has issued a regulation affecting security in fixed guideway rail transit systems. Pursuant to 49 CFR Part 659, Rail Fixed Guideway Systems; State Safety Oversight,²⁰ rail fixed guideway systems,²¹ not regulated by FRA as a railroad, must maintain a system security plan that meets specific parameters and conduct internal security reviews of the implementation and effectiveness of the security plan. FTA administers this regulation, which also requires a system safety plan, through State Safety Oversight Agency (SSOA), these are required to ensure transit systems under their responsibility conduct an annual review of their system security program plan²² and to develop and document a process for conducting ongoing assessments of implementation of the system security program plan.²³ Covered rail transit systems must complete these assessments of all required elements of their system security program plan over a three-year cycle. Each SSOA is required to perform an on-site review of implementation of the system security program plan at least once every three years.²⁴

FRA maintains regulatory authority for rail safety over commuter rail operators and Amtrak. The agency employs a force of several hundred rail inspectors that monitor the implementation of safety and emergency preparedness plans at these systems. In accordance with 49 CFR Part 239, railroads operating or hosting intercity or commuter passenger train service must “adopt and comply with a written emergency preparedness plan approved by FRA.”²⁵ The plan must include specific elements and procedures for implementation, covering the following areas:

- Crew member assessment of a passenger train emergency and prompt notification to the control center;
- Control center notification to outside emergency responders;
- Employee training and qualification on the emergency preparedness plan for on-board personnel and control center personnel;
- On-board emergency lighting;
- Maintenance of on-board first aid kits and emergency equipment;
- Passenger safety awareness of emergency procedures; and
- Conduct of passenger train emergency simulation to determine capabilities to execute the emergency preparedness plan with after action debriefing and critiques.²⁶

The regulation also sets specific requirements for marking of emergency exits and for the inspection, maintenance, and repair of these exits.

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. As indicated above, State oversight agencies audit compliance with the FTA's regulations on system safety and security plans in rail fixed guideway systems. Additionally, State and local governments may 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. The responsibility for responding to emergencies involving the mass transit and passenger rail infrastructure often falls to State and local governments.

²⁰ 49 CFR § 659.

²¹ 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.

²² See 49 CFR § 659.25.

²³ See 49 CFR § 659.27.

²⁴ See 49 CFR § 659.29.

²⁵ See 49 CFR § 239.101(a).

²⁶ See 49 CFR § 239.101 through 239.103.

Mass transit and passenger rail operators, which can be public, private, or semi-private entities, are responsible for administering and managing public transportation services and related activities, including security. These agencies can directly provide security, through an inherent law enforcement department or security contingent, or contract with outside law enforcement departments or security firms to provide security in the mass transit or passenger rail system. 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 rail and bus systems rests with the operators.

TSA continues to work closely with all its public and private security partners to ensure that all gaps, fragmented efforts, and unnecessary redundancies and overlaps in security roles and responsibilities are identified and addressed. In some cases, this effort has entailed producing a memorandum of understanding (MOU) with a governmental partner. The Public Transportation Annex to the September 2004 DHS/DOT MOU, executed in September 2005 by TSA, FTA, and DHS's former Office of State and Local Government Coordination, is an example of this type of coordination. The Annex is subject to annual review to ensure its continued effectiveness in delineating roles and responsibilities between TSA and FTA. Other examples are the memoranda of agreement completed with mass transit and passenger rail agencies in connection with pilot testing of security technologies and the operations plans produced to govern joint security operations conducted by TSA with mass transit and passenger rail agencies through deployments under the VIPR program. Through these types of cooperative efforts, respective roles and responsibilities are now more clearly defined and security partners work in a collaborative environment to ensure that security gaps are mitigated and a high level of security is achieved and maintained in mass transit and passenger rail systems.

2.3.3 Security Risk

The attributes of mass transit and passenger rail systems essential to their efficiency also create potential security vulnerabilities that terrorists seek to exploit. Unlike air transport, where strict access controls and universal security screening apply, public transportation operates more openly, in fast-paced operations with numerous entry, transfer, and egress points, to transport a high volume of passengers every day that greatly exceeds the number of air travelers. Multiple stops and interchanges lead to high passenger turnover, which is difficult to monitor effectively. The broad geographical coverage of mass transit and passenger rail networks provide numerous options for access and getaway and afford the ability to use the system itself as the means to reach the location to conduct the attack. This tactic has been used to great effect in successful terrorist attacks overseas on rail and bus systems, most notably the April 1995 sarin attacks on the Tokyo subway system; the multiple detonations of improvised explosive devices (IEDs) left on commuter trains in Madrid in March 2004; the multiple suicide attacks employing IEDs on the London Underground and a double-decker bus in London in July 2005; and the multiple detonations of IEDs on commuter trains in the greater Mumbai area in July 2006.

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, local, and tribal governments. A potential terrorist attack on public transportation systems can result in a large number of victims, both killed and wounded, as well as significant property damage. The recent examples of the Madrid, London, and Mumbai bombings—all involving use of multiple IEDs—are tragic reminders of this reality. The possibility of an attack in the United States remains real, as evident in the 2009 Al-Qaeda attempt to detonate explosives on the New York City subway system. Najibullah Zazi, a legal permanent resident of the United States, was arrested and accused of planning suicide bombings on the subway during rush hour as one of three coordinated attacks in an Al-Qaeda plot. He had undergone training at an Al-Qaeda camp in Pakistan in 2008. Zazi was arrested before he could carry out the attacks. Since then, he and two other defendants have pled guilty to conspiracy to use weapons of mass destruction.

The consequences of an attack are related to 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. A transit bus explosion in a crowded highway tunnel could have dire consequences, as well. 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, which are 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 its tunnels, moving trains, and ventilation shafts, can facilitate distribution of a chemical or biological agent throughout its facilities and affect other areas of a city because of exterior vents and station egress points.

Other potential include a vehicle bomb near a station or track, explosives on a track, or an IED or a lower-yield explosive in a station, train, or bus. Detonation of conventional or improvised explosives will likely result in scores of casualties. In addition to loss of life, consequences of 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 continuity of government operations.



3. Implementation Plan

3.1 Strategies and Objectives

The SSP identifies a set of goals and objectives for the Transportation Systems Sector. Achieving these goals and objectives requires a strategic approach that integrates the needs and requirements of the industry through meaningful collaboration. 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 SSP goals and objectives and employ risk-informed decisionmaking to determine specific actions.

Figure C3-1 below demonstrates the process model culminating in mass transit and passenger rail security programs and initiatives.

Figure C3-1: Process Model



The plan to enhance security in public transportation is focused on:

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

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. TSA pursues continuous engagement with senior executives, law enforcement chiefs, and security managers for mass transit and passenger rail agencies; State, local, and tribal government officials, law

enforcement, and emergency responders; and Federal partners to foster regional security coordination and to integrate the spectrum of available resources for enhanced deterrence and response capabilities.

Collaboration in the identification of security enhancement and grant funding priorities occurs through joint Regional Transit Security Working Groups for high risk areas, specifically Boston, New York, Philadelphia, the National Capital Region, Atlanta, Chicago, Los Angeles, and San Francisco. TSA further facilitates consultations on strategic priorities, program development, and operational initiatives with the Transit Policing & Security Peer Advisory Group (PAG), a forum of long-serving law enforcement chiefs and security directors for mass transit and passenger rail agencies across the Nation. TSA also uses annual Transit Security Roundtables, which help to join law enforcement chiefs and security directors for Amtrak and the largest 50 mass transit and passenger rail agencies with Federal security partners in focused discussions of specific challenges in terrorism prevention and response to share experiences and advance collaborative solutions.

3.1.2 Continuously Advancing the Security Baseline

The Surface Transportation Security Inspection Program (STSIP), through inspections, assessments, and technical assistance, together with the systems' self-assessments, and other efforts by government and industry partners continue to help advance security baselines and enhance security posture throughout the passenger rail and mass transit mode. TSA's TSIs are assigned to cover the key rail and mass transit facilities in 20 metropolitan areas around the country. Beyond conducting security assessments and evaluating compliance with security requirements, inspectors serve as TSA's regional liaison to mass transit agencies and their Federal, State, local, and tribal security partners.

TSA has implemented a continuous improvement process via comprehensive security assessments conducted by TSIs under the BASE program. These assessments evaluate posture in 17 Security and Emergency Management Action Items foundational to an effective security program. The action items were developed by FTA in the aftermath of the attacks of September 11, 2001, and enhanced in 2007 in a cooperative effort by TSA and FTA with input from the mass transit and passenger rail operating and security officials engaged through the Mass Transit SCC and Transit Policing and Security PAG. The results inform security enhancement priorities and review of projects under TSGP for mass transit and passenger rail agencies. In 2008, TSA transformed the assessment results into smart security practices developed and implemented by the assessed agencies. TSA has disseminated these practices with contact information for the implementing agencies to transit security professionals, and these practices can be adapted to operating circumstances in other systems.

Since the inception of this program in 2006, TSA has completed over 100 BASE assessments and reassessments, covering the majority of the largest 100 agencies and some smaller systems. The overall average score on all 17 Action Items indicated solid performance for the first round of the most thorough security assessments agencies have yet undergone. However, TSA originally set a high performance standard – the DHS Annual Performance Report measure for this area originally set a standard of 90 percent average score across 17 Action Items, with no category under 70 percent. While the largest 50 mass transit and passenger rail agencies are being reassessed to directly evaluate improvement, the standard is being readjusted. Three levels of security will be considered to reflect the risk-informed approach of BASE:

- a) If a transit agency achieves a BASE score of 90% or greater with no one Action Item less than 70%, then they are scheduled for the next BASE in three years, and are considered to have achieved the Gold Standard;
- b) If a transit agency achieves a BASE score between 70% - 89% with no one Action Item less than 70%, then they are scheduled for the next BASE in two years, and are considered to be In Compliance; and
- c) If a transit agency achieves a BASE score of less than 70% then they are scheduled for the next BASE the following year, and they are considered to be Not in Compliance. These properties will be visited on a regular basis until they are In Compliance and will have a Performance Improvement Action Plan on file at TSA.

The strategic objective of this program is twofold; elevate performance to this high standard among higher risk agencies and reduce risk scores through continuing assessments and security support to improve performance. Assigned in metropolitan areas whose mass transit and passenger rail agencies provide services to the overwhelming majority of users of public transportation across the Nation, the TSIs are well-positioned to play this role. While continuing the BASE assessments, the currently authorized force of approximately 400 inspectors serves as direct liaison to mass transit and passenger rail security officials. In this capacity, they facilitate security enhancement efforts, respond to reports of threats and suspicious incidents, and foster regional security collaboration. Because of the need for a consistent and collaborative engagement within each region of the country, the SCC is of the view that the TSIs with responsibility to assist with mass transit security should report to the Mass Transit Division.

3.1.3 Building Security Force Multipliers

TSA continues its persistent effort aimed at expanding informed, capable “eyes and ears” for security through targeted awards under the TSGP for employee security training, anti-terrorism exercises, public awareness campaigns, and fielding specially-trained and equipped anti-terrorism law enforcement teams and technological systems to enhance detection and deterrent capabilities.

The total risk-based TSGP investment in mass transit and passenger rail security for the period of FY 2006 through FY 2009, including the supplement under the American Recovery and Reinvestment Act of 2009, is approximately \$1.5 billion. The economic stimulus legislation adds another \$150 million. Enhanced infrastructure protection is achieved through grant funding of visual surveillance and monitoring, intrusion detection, access control, and explosives detection systems. TSA’s Mass Transit Security Training Program targets grant funds to recurrent training of law enforcement officers and frontline employees in core areas of security awareness, behavior recognition, and immediate response to a threat or incident. TSA’s “Not On My Shift” initiative produces posters and tip cards for frontline employees emphasizing the critical importance of their vigilance, observations, and reporting in terrorism prevention and provides products tailored to the agency with its logo, system images, and employees’ quotes.

Through the Intermodal Security Training and Exercise Program (I-STEP), TSA employs multi-phased workshops, tabletop exercises, and “lessons learned” working groups to integrate mass transit and passenger rail agencies with regional law enforcement and emergency response partners to expand and enhance coordinated deterrence and incident management capabilities. Multiple I-STEP exercises have been conducted and others are scheduled. This program expands upon the coordinated regional effort advanced through the “Connecting Communities” public transportation emergency response forums, which are conducted on average eight times per year by TSA and FTA at varying locations.

3.1.4 Providing Security Information Leadership

A robust information sharing strategy continues to be central to TSA’s approach to securing the Nation’s mass transit and passenger rail systems. This strategy focuses on the capability to collect, analyze, integrate, and disseminate to decisionmakers for action an uninterrupted flow of information. It 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; undercutting attack preparations and minimizing the consequences should an attack occur.

TSA continues to employ a multi-faceted effort to bring timely, accurate intelligence and security information to mass transit and passenger rail agency officials. A joint DHS Office of Intelligence and Analysis, TSA Office of Intelligence (TSA-OI), and FBI effort provides classified intelligence and analysis to mass transit and passenger rail security directors and law enforcement chiefs in 16 metropolitan areas simultaneously through the Joint Terrorism Task Force (JTTF) network’s secure video teleconferencing system. These briefings advance two key strategic objectives—providing intelligence and security information

directly to mass transit and passenger rail law enforcement chiefs and security directors and advancing regional collaboration by bringing these officials together with their Federal partners to discuss the implications for their areas and coordinate to implement effective security solutions.

To facilitate immediate communication of classified intelligence, TSA has deployed secure telephone equipment to Amtrak and agencies ranked among the largest 20 in passenger volume and regionally through secure cell phones maintained by TSIs assigned in major metropolitan areas. A dedicated Alert Notification System, which includes regularly updated rosters of Federal security partners and security and management officials of mass transit and passenger rail agencies, ensures immediate notification of potential or actual threats and security incidents. Multiple address lists enable communication access to agencies based on size, geographic location, categories of officials, type of system, and nature of infrastructure.

Finally, TSA periodically disseminates Security Awareness Messages to a group of mass transit and passenger rail security and management officials and State and local partners. These messages distribute DHS, FBI, and TSA intelligence products with security context relevant to mass transit and passenger rail operations. In each message, TSA cites recommended protective measures and discusses use of the accompanying materials, which include intelligence products and training aids, in training and awareness activities.

3.1.5 Deploying Tools to Mitigate High Consequence Risks

TSA drives security grant funds to high risk systems for training, operational deterrence, and key infrastructure protection. Our strategic priority of active deterrence is advanced through random security inspections and coordinated, joint random security surges, supported through TSGP awards. As noteworthy examples of progress in implementation, several mass transit and passenger rail agencies have implemented or approved programs for random inspections of passenger bags, randomly integrating TSA screening expertise through the use of VIPR teams. Amtrak and TSA jointly planned and executed the largest coordinated rail security operations yet conducted in the United States in the heavily traveled Northeast Corridor. Through Operation ALERTS (Allied Law Enforcement for Rail and Transit Security), unannounced security surges simultaneously deploy law enforcement officers from nearly 150 departments to more than 150 Amtrak and commuter rail stations from Richmond, Virginia, to Portland, Maine. These operations unify State and local law enforcement departments with Amtrak Police and police and security forces for regional commuter railroads and transit systems throughout the Corridor, greatly expanding the scale of resources available for random, unpredictable security activities that are essential to deterrence. This coordinated effort enables both simultaneous region-wide surges and more frequent, random patrols and joint operations on a localized level.

Mass transit and passenger rail agencies across the country coordinate and execute similar operations on a random, unpredictable basis. As representative examples, these efforts include:

- Multi-Agency Security Sweeps (MASS) coordinated by the New York Police Department (NYPD) and New York Metropolitan Transportation Authority (NY MTA) to deploy police officers and security officials from multiple agencies simultaneously in random, unpredictable security surges. Participating agencies include the Amtrak Police Department, Port Authority Police Department, New Jersey Transit Police, TSA through VIPR teams, and National Guard personnel deployed for security activities in New York City.
- Randomly deployed Train Order Maintenance Sweeps (TOMS), used extensively by NY MTA in partnership with the NYPD and New Jersey Transit Police in a coordinated effort with county and local law enforcement departments throughout the New Jersey Transit commuter rail network, surge uniformed police officers to platforms to board and conduct security inspections on arriving trains.
- Transit Shield deployments in the Miami-Dade Transit system, which randomly deploy details consisting of Miami-Dade Police officers, Metrorail security officers, members of the Miami-Dade Transit Office of Safety and Security, and TSA personnel in security patrols and sweeps.

- Joint operations by the Los Angeles Sheriff's Department with the Los Angeles Metropolitan Transportation Authority and Metrolink regional commuter rail to conduct random inspections of passengers' bags throughout the systems.
- Coordinated extension of normal law enforcement jurisdiction by Long Beach Police Department Transit Enforcement Officers (LBPD-TEOs) to the 13 cities and jurisdictions served by Long Beach Transit buses while maintaining cooperative efforts for security activities, response calls, and other police services.

TSA supports implementation of random, unpredictable security activities intended to form changing layers of security through multiple means. VIPR deployments augment security capabilities for random patrols and surges, behavior detection, and explosives detection through canine teams and Explosives Security Specialists. Continuing risk-based deployment of TSA-certified explosives detection canine teams expand systems' deterrence and detection capabilities. Also, eligible mass transit and passenger rail agencies may procure equivalently trained and certified canines as a priority under the TSGP.

Coordinated technology development and testing in partnership with the DHS Science and Technology Directorate (S&T) focuses on enhancing capabilities to protect high risk assets and systems, notably underwater tunnels and high volume terminals and stations, and to detect and deter terrorist activity and prevent attacks in the transit environment. Ongoing projects include: the resilient tunnel program, a high impact technology solutions project specifically pursuing novel means to protect critical transportation tunnels; anomalous explosives detector for surface transportation; intelligent video monitoring at mass transit sites; bus and train command and control; chemical/biological program for mass transit; explosives testing and assessment of rail car vulnerability; mass transit tunnels entry denial systems; and rapid response to extreme events in tunnels.

These initiatives are informed through assessments. As a condition of grant eligibility, mass transit and passenger rail agencies must undergo risk assessments coordinated and funded through the precursor to the FEMA's National Preparedness Directorate. DHS Office of Infrastructure Protection's (IP) Protective Security Advisors conduct thorough risk assessments in critical infrastructure throughout the Nation, some of which cover key mass transit and passenger rail terminals and stations. TSIs assess the systems' security plans, programs, and measures to identify concerns and improve effectiveness.

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 table C3-1, are designed to achieve enhanced security by providing flexible, mobile, and fixed technological means to facilitate the process.

Table C3-1: 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 (Federal Security Directors (FSDs), Federal Air Marshal Supervisory Agents in Charge (FAMSACs), lead regional TSIs, 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"> • Focus resources and efforts towards hardening the Nation's most critical mass transit and passenger rail assets.
<ul style="list-style-type: none"> • Conduct Security Readiness Assessments through collaborative efforts between area Surface Inspectors and transit security officials to conduct security assessments under the BASE program.

Mass Transit Objectives

- Coordinate with system security officials to examine the capabilities of transit agencies and front-line employees in identifying and reporting suspicious items and activities.
- Improve Intelligence and Security Outreach through coordination among TSA-OI, the TSA Mass Transit Division, TSIs, and the regional intelligence and information-sharing centers to implement through regional engagement.
- 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.
- Employ all available media—public address system announcements, billboards and posters, brochures, and memorabilia 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 Strategic Risk

Critical systems and assets have been identified via a collaborative effort involving TSA and other components within the DHS, FTA, FRA, 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 systems and assets. In support of TSA's Transportation Sector Security Risk Assessment (TSSRA), an overarching, strategic, scenario-based cross-modal risk assessment based on threat, vulnerability, and consequences, TSA has developed a criticality-based assessment tool designed to further inform DHS leadership of security priorities, support strategic risk analysis process, and help security experts prioritize mass transit assets. The output of the criticality-based assessment tool is an important component to determining vulnerability scores for the TSSRA.

3.3 Tactical/Operational Risk

TSA is currently developing technologies to provide several risk and vulnerability assessment products based on commercial off-the-shelf risk assessment software. In mass transit, the STSIP has developed and fielded a module for BASE – assessing security in transit, commuter, and passenger rail systems. Modules currently under development for the mode include:

- Mass Transit Risk Assessment – tool to assess risk to mass transit systems
- Under Water Tunnel Assessment – tool to assess security for transit systems that operate in underwater tunnels
- Station Profiles – tool to assess physical security measures at mass transit and other surface transportation stations
- System Observations – tool to capture TSI observations of security practices in mass transit systems

TSA is also developing a program for transit and passenger rail operations to supplement their BASE assessment and other risk assessment tools currently being developed. The program includes a tactical and operational risk assessment tool that transit agencies will be able to use to conduct self-assessments. The tool identifies all the system's assets and each assessment will define specific outcomes in response to various risks. Various countermeasures will then be applied to potential direct and indirect consequences of a terrorist attack to evaluate the countermeasures' effectiveness. Risk reduction strategies will be devised to address the greatest return on investment for mitigation.

The program will begin as a tool available to new operations for use in pre-service risk assessment and to those operations that may be involved in a National Security Special Event. It will include training for the agency personnel in using the tool as well as follow-on support, and will grow with interest and as resources become available.

3.4 Security Programs and Processes

3.4.1 Surface Transportation Security Inspection Program

The 9/11 Act has multiple requirements pertaining to mass transit and passenger rail best coordinated through, overseen by, and executed with TSIs experienced in the mode. These demands expand upon the existing wide-ranging efforts the TSIs undertake in advancing TSA's strategic priorities for mass transit and passenger rail security. Specific areas include:

- Target assessments of the relevant security areas as the regulations required by the 9/11 Act are developed.
- Implement plans, assessments, and training programs to ensure TSA produces requirements that build upon existing practices and elevate the baseline.
- Once proposed rules are published, assist covered mass transit and passenger rail agencies with aligning their security plans, assessments, and training programs to pending requirements.
- Conduct substantive review, note any corrective action needed, and forward recommendations to meet a 9/11 Act requirement that DHS review and approve the security plans and security training programs of covered mass transit and passenger rail agencies.
- Perform compliance inspections to verify that security plans, employee training programs, and threat assessment requirements are being implemented consistently with their provisions and in accordance with requirements of the applicable regulations.
- Coordinate with mass transit and passenger rail agencies and regional security partners to conduct the multi-phased terrorism prevention and immediate response exercise program in development to meet a 9/11 Act requirement to produce a national exercise program for mass transit and passenger rail.
- Participate with mass transit and passenger rail agencies to execute joint public awareness exercises of the national public awareness program to meet a 9/11 Act requirement to develop and implement a national public awareness program for mass transit and passenger rail.
- Following publication of the relevant proposed rules, create a BASE assessment checklist that integrates the 9/11 Act requirements.
- Continue BASE assessments on all of the 100 largest mass transit and passenger rail agencies and conduct second assessments on the top 50 to meet 9/11 Act requirements that address security assessments both in terms of the security plans required by regulation and in terms of the authorization of the STSIP.
- Build on existing regional security liaisons to expand partnerships and resources available for the random, unpredictable security activities vital to deterrence of terrorism.
- Assume a more active role in oversight of projects funded by the TSGP, particularly with respect to operational activities, such as funded anti-terrorism teams (Op-Packs), training, exercises, and public awareness activities, which are eligible under the 9/11 Act grant authorizations.
- Involve TSIs in the coordination, planning, preparation, and execution of VIPR deployments as authorized by the 9/11 Act (recognizing FSDs and FAMSACs lead the regional TSA team, while leveraging the relationships TSIs have built with security

professionals in the mass transit and passenger rail systems, which make them ideal to play a prominent role, especially as VIPR operations assume a more regional focus).

- Identify the frequencies and types of communications used by mass transit and passenger rail agencies to coordinate security activities and emergency response in order to advance interoperability for VIPR deployments.
- As resources permit, provide training to designated employees of mass transit and passenger rail agencies in behavior recognition via the Terrorist Activity Recognition and Reaction (TARR) course on a train-the-trainer basis, with emphasis on 1) grant-eligible systems that are facing significant delays in receiving this training through an approved provider or 2) systems not eligible for support under the TSGP.

Effective development and implementation of TSA's security strategies, plans, and programs depend upon close coordination and collaboration between TSIs and the Division. This unity of effort has made the substantial progress already achieved in security enhancement possible and is essential to the continuous effort to expand terrorism prevention and response capabilities in mass transit and passenger rail agencies throughout the Nation. For accomplishment of TSA's security mission in this mode, and particularly to assure the continued advancement of innovative solutions to security challenges, the synergistic effect resulting from the integration of the collective expertise and experience in the Division and the Inspection Program will be maintained.

3.4.2 VIPR Teams

As part of implementing flexible, layered, and unpredictable security programs using risk management principles, the VIPR 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 VIPR teams provide TSA and the transit and passenger rail agencies with the ability to leverage a variety of resources quickly and effectively.

Depending on the specific needs of the systems to which they are deployed, the teams consist of any combination of FAMs, TSIs, TSA-certified explosives detection canine teams, Behavior Detection Officers, Bomb Appraisal Officers, 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.

More than 900 VIPR operations were conducted in mass transit and passenger rail systems since the program's inception in December 2005, with dramatically increased pace over the past two years. VIPR teams work with local security and law enforcement officials to supplement existing security resources, provide deterrent presence and detection capabilities, and introduce elements of randomness and unpredictability to disrupt potential terrorist planning activities. To enhance coordination and deterrent effects, TSA and the representatives of the Transit Policing and Security PAG worked cooperatively and closely to improve coordination, preparation, planning, execution, and after-action review of VIPR deployments in mass transit and passenger rail systems. This cooperation culminated with the completion of mutually agreed upon operating guidelines for "Effective Employment of Visible Intermodal Prevention and Response Teams in Mass Transit and Passenger Rail." The guidelines were distributed to FSDs, lead regional TSIs, and FAMSACs around the country to improve the effectiveness of the VIPR program. A follow-on product, developed and distributed in 2008, details the roles and capabilities of the multiple TSA resources available to participate in VIPR deployments and provides recommendations on effective deployment in anti-terrorism activities. Additionally, TSA recently developed and distributed an informational tool kit to assist transit and other modes in planning and conducting VIPR operations. The kit includes an informational pamphlet and DVD on VIPR components.

Consistent with the strategic plan for regional VIPR deployments in mass transit and passenger rail venues, national and regional level VIPR deployment planning occurs simultaneously, integrating the teams with other available regional, State, tribal, and local resources. More frequent regional deployment of VIPR teams enhances the deterrent effect. Continued oversight at the national level will advance the development of surge capacity and will ensure effective employment of TSA security resources.

3.4.3 Information-Sharing

The Federal Government continues to coordinate overall communications with its security partners using a number of tools and processes for the sharing of both classified and unclassified information. These tools and processes include:

Information Sharing and Analysis Center—The 9/11 Act directed DHS to provide operating funds for the Public Transit - Information Sharing and Analysis Center (PT-ISAC) in order to provide an industry focused 24-hour/7-day-a-week information sharing capability. The PT-ISAC, supported by analysts who search secure and open sources and communicate security-related information and advisories to public transportation systems, works with TSA and the intelligence community members to provide significant unclassified threat and situational awareness information to the mass transit and passenger rail community. Congress also directed TSA to develop a TS-ISAC to support the transportation-focused ISACs. Where applicable, the HSIN-CS portal acts as the platform that coordinates efforts across the critical sector ISACs, including transportation. Along with the PT and TS ISACs, TSA-OI and the Division are looking to involve other emerging technologies/information systems (such as the FBI's e-Guardian system) to develop an efficient analytical process that will allow for timely review and dissemination of Intelligence Reports and Suspicious Incident Reports that could include embedded TSA security-related comments. The development of this process, still in its early stages, could have a significant impact on the reporting process for suspicious incidents and on information sharing among transit and passenger rail agencies across the country.

Joint Terrorism Task Force Classified Threat Briefings—Since the initial issuance of this plan, TSA has continued to coordinate with the FBI's JTTFs to access the FBI's secure video teleconference capabilities located throughout the United States, enabling delivery of national and regional classified threat briefings to transit systems' security and operations officials. These Joint DHS/TSA/FBI threat and analysis briefings at the Secret level, held on a semi-annual basis, bring together mass transit and passenger rail security directors and law enforcement chiefs with their Federal security partners in as many as 19 metropolitan areas through the secure video teleconferencing system maintained in the JTTF network. This capability enables timely assembly of these key officials through this means for unscheduled sessions as threats or security incidents warrant.

Secure Phone and Private Industry Security Clearance Program—TSA has also continued to distribute and support secure phones for the largest transit and passenger rail agencies and has enhanced its industry security clearance program to ensure there are security representatives at the key agencies that possess Secret security clearances.

3.4.4 Security Training and Awareness

Targeted Security Training Initiative—The BASE assessment results indicated a need for more focused effort in security training for mass transit and passenger rail agencies' employees. Although an extensive Federal security training program has been implemented since the attacks of September 11, 2001, training thousands of transit employees, 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. 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. Many of the training courses are federally sponsored and continue to be funded in part by the FTA as well as by TSA. Presented in a readily understandable matrix, the program 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. TSA has also partnered with FTA to advance the Mass Transit Security Training Program, providing the mass transit community with expanded opportunities to enhance their training programs.

Connecting Communities—This initiative, which brings the Federal transportation security partners together with State, local, and tribal government representatives and the local first responder community to discuss risk reduction and response efforts and ways to work together effectively to prepare and protect their communities, continues to be a success. TSA partners with FTA on Connecting Communities.

Security and Safety Roundtables—TSA, FTA, and the Federal Emergency Management Administration/Grants Program Directorate (FEMA/GPD) partner in Transit Security and Safety Roundtables. The roundtables bring together the security coordinators and safety directors from the Nation's 50 largest mass transit and passenger rail agencies and facilitate dialogue between the government, industry leaders, and police, safety, and security departments on how best to address current transit safety, security, and emergency management challenges. The roundtables provide a forum for the agencies' safety and security officials and their Federal government counterparts to share effective practices and develop relationships to improve coordination and collaboration. Roundtables occur annually.

3.4.5 National Tunnel Security Initiative

In October 2006, TSA led the formation of an Interagency Tunnel Risk Mitigation Working Group. This group brought together experts consisting of representatives from the DHS S&T, IP, Office of Intergovernmental Affairs, FEMA, FTA, and the JTTF. The overall strategic risk reduction objective of this working group was to identify the means to reduce the likelihood and impact of a catastrophic breach of an underwater mass transit tunnel due to terrorist attack. Robust engagement with stakeholders was critical to this strategy.

This strategy was guided by four primary objectives:

- Improve information sharing and guide transit security grant projects related to preventing and mitigating risk to underwater transit tunnels;
- Complete structural modeling for tunnels requiring assessment;
- Prioritize tunnel structures requiring risk mitigation; and
- Identify, through research and development, viable mitigation strategies.

Over the last few years, the Tunnel Working Group has been executing this strategy. Transit properties with underwater tunnels have received significant funding through the TSGP to implement operational measures, such as canine teams, random patrols, and closed-circuit television (CCTV). Additionally, TSA and S&T continue to collaborate on several research and development initiatives, including the resilient tunnel project, testing different materials for liners in tunnels.

3.4.6 Security Technology Deployment

This cooperative initiative between TSA and mass transit and passenger rail stakeholders deploys various security technologies to interested public transportation systems as security supplements and for 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 S&T and the TSA Office of Security Technology, 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.

3.4.7 Technology Research and Development

Public and private partners are working together to evaluate technology needs of the 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. 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 through: the Transit Safety and Security Roundtables discussed earlier; direct outreach to the Transit Policing and Security PAG and the Transit, Commuter, and Long Distance Rail GCC; the Mass Transit SCC; requirements workshops; interagency informational tours; and other meetings. The results are developed into broad requirements submitted to S&T for research and development. Furthermore, TSA participates in the Integrated Project Teams (IPTs) held by S&T across a variety of functional areas. These IPTs provide a means to submit technology requirements for funding and coordinate requirements with other DHS internal stakeholders (i.e., Customs and Border Protection, United States 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 continues to post applicable technology reports to the HSIN-Public Transit Portal.

3.4.8 International Initiatives

TSA continues to maintain extensive engagement with foreign counterparts on transit security with the aim of sharing and glean 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 European Union, the Asia Pacific Economic Cooperation (APEC), UIC Security Conferences, and the Mexican and Canadian governments fosters sharing of effective practices and technologies in mass transit and passenger rail security. The International Working Group on Land Transport Security (IWGLTS), which formed to provide a global forum for experts to share best practices and lessons learned, continues its focus on passenger rail and mass transit security. TSA assumed the one-year chairmanship of this working group in 2008 and hosted a meeting in November 2008 in San Francisco and another one in May 2009 in Los Angeles. The group's efforts thus far have led to several beneficial studies in mass transit and rail security, including in the areas of public awareness and recovery from an attack or incident involving chemical, biological, or radiological weapons and hazards. The two working group meetings hosted by the United States resulted in five sub-working groups examining a broad range of security areas that will allow for the continuing sharing of smart practices and initiatives. These areas include Public Awareness, Mitigating/Smart Practices, Technology, Security Assessment, and Outreach.

Through the Joint Contact Group, the United States and the United Kingdom continue their bilateral cooperation 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.

TSA is also participating in the Congressionally-sponsored Transportation Security Centers of Excellence (COE) program which is being sponsored by S&T. Under this effort, TSA is partnering with DHS, Transit Agency subject matter experts, COE representatives from several colleges and training institutions to develop a Bus Operator Awareness/Research and Development initiatives evaluation program. Part of this effort to expand security awareness principles was a trip of a team of experts to visit international security partners in Israel and England where security-related effective practices and concepts were exchanged.

3.4.9 Grant Programs

Through the TSGP, DHS funds security enhancements in mass transit and passenger rail agencies in a risk-based approach. During FY 2009, eligible mass transit systems received \$348.6 million in TSGP funds as well as \$25 million to Amtrak. The

American Recovery and Reinvestment Act grant supplemental in 2009 provided \$150 million in additional funds to hire transit security officers and fund capital security projects for both Tier I and II eligible transit agencies. During FY 2008, the total allocation was \$356 million to eligible mass transit and passenger rail systems plus \$25 million to Amtrak. Total funding under the program in FY 2007 reached \$255 million through the annual DHS appropriation and the supplemental.

The TSGP employs risk-based prioritization consistent with this SSP. This approach applies TSGP resources to generate the highest return on investment and, as a result, strengthens 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 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 agency and regional risk, the efficacy of the project in reducing risk, cost effectiveness, and the ability to complete the proposed project with the funds awarded. Ferry systems are also eligible to apply if they are in a Tier I region.

Since the inception of the TSGP, TSA has worked diligently to make the grant process more efficient. It has since succeeded in implementing a series of measures, including reducing the time frames by streamlining the process and clearly defining FEMA's and TSA's roles and responsibilities. TSA and FEMA conducted a comprehensive stakeholder outreach to gather input on improving the processes. This resulted in significant improvement by both agencies. TSA continues to implement additional means, including increased accountability and tracking, to further streamline the process. Mass Transit SCC has provided comment for inclusion in this plan stating that the grant program should be fully managed by the Division without FEMA review/approval, and the process needs to be further streamlined.

3.5 Effective Practices, Security Guidelines, and Security Standards

3.5.1 Security Guidelines

In February 2008, TSA issued additional guidance on background checks, redress, and immigration status. Item 14 of the Security and Emergency Management Action Items (established jointly by TSA and FTA) recommended that the operators of mass transit entities conduct background investigations, such as criminal history and motor vehicle records, on all new front-line operations and maintenance employees and those employees and contractors with access to sensitive security information and security critical facilities and systems. Furthermore, the protective measures recommended by TSA and FTA for threat level Green (Low), include measure 2.16 to "perform background checks on all employees and on contractors consistent with applicable law." The additional guidance issued by TSA contains further guidance on the factors to consider on the recommended scope of and procedures for voluntarily conducted background checks.

In March 2009, FTA issued a guidance document called "Sensitive Security Information (SSI): Designation, Markings and Control, Resource Document for Transit Agencies." It is devised to help transit agencies prevent the unauthorized disclosure or dissemination of SSI, while preserving the public's right to know about transit systems and operations. This document can be used as a resource in developing policies and procedures for identifying, marking, and handling SSI in order to control access to it.

3.5.2 Security Standards Development

TSA and its Federal partners continued their engagement with APTA's Security Standards Policy and Planning Committee to develop recommended practices to enhance security in transit systems. 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 through the GCC/SCC framework and Critical Infrastructure Protection Advisory Council (CIPAC) process to develop consensus-based standards to enhance security in transit systems. TSA has provided subject matter

expertise to the joint working groups, which cover three areas: infrastructure protection, emergency management, and security risk management.

This initiative has produced the following six published standards:

- Recommended Practice for a Continuity of Operations Plan
- Recommended Practice for First Responder Familiarization of Transit Systems
- Recommended Practice for Security & Emergency Management Aspects of Special Event Service
- Recommended Practice for Trash/Recycling Container Placement to Mitigate the Effects of an Explosive Event
- Recommended Practice for CCTV Camera Coverage and Field of View Criteria for Passenger Facilities
- Recommended Practice for the Development and Implementation of a Security and Emergency Preparedness Plan

3.5.3 Rulemaking

On November 26, 2008, TSA published a final rule on Rail Transportation Security (49 CFR Parts 1520 and 1580), with an effective date of December 26, 2008. While the bulk of security requirements in the regulation pertain exclusively to freight railroad carriers, rail hazardous materials shippers, and rail hazardous materials receivers, three elements apply to passenger rail operations: TSA's inspection authority, appointment of a Rail Security Coordinator, and reporting of significant security concerns to TSA. These requirements apply to passenger rail carriers generally, including intercity passenger railroads, commuter railroads, and rail transit systems (subways and light rail).

The Division and TSIs continue to work with the industry to ensure the awareness and implementation of these requirements. TSA has implemented a process to receive, analyze, evaluate, and synthesize incident reports, and TSIs liaise with the operators to ensure proper incident reporting and accurate and current reporting of security coordinator information. The requirements have now been integrated into the BASE assessment checklist.

The 9/11 Act directed DHS to issue regulations requiring public transportation agencies and passenger rail carriers to develop and implement security plans (sections 1405 and 1512) and security training programs for frontline employees (sections 1408 and 1517). The Act also directed DHS to conduct threat assessments of all public transportation frontline employees. Consistent with the 9/11 Act requirements, TSA is developing a proposed rule for security training programs and is engaged in consultations with stakeholder groups, notably the Mass Transit SCC and the Transit Policing and Security PAG. TSA is following a similar approach in development of the security plan regulation.

Fostering development of the security training program regulation is the work TSA had already completed, six months prior to enactment of the 9/11 Act, in producing the mass transit and passenger rail security training program guidelines and implementing the focused security training initiative under the TSGP.

Finally, to meet the requirements of sections 1411 and 1520, work is ongoing to draft a rule to implement the 9/11 Act requirement to conduct name-based checks on public transportation and passenger rail frontline employees against the terrorist watch list and immigration status.



4. Metrics

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 have been developed and are being monitored. These measures supply the data to affirm that specific goals are being met or to show what corrective actions may be required.

These measures of effectiveness are based on TSA's assessment and evaluation of security posture of the mass transit and passenger rail modes through the BASE program. Security assessments commenced during FY 2007, with a focus on the 50 largest mass transit and passenger rail agencies based on passenger volume.

TSIs conduct BASE assessments alongside members of the transit system being assessed. This process can take a few days up to a few weeks, depending on the system's size. TSIs work through each of the assessment categories and determine the overall score using a 5-point scale from 0 to 4. They use a standard checklist to ensure that each transit system is assessed and scored on the same criteria. The basis for each score assigned is documented in supplementary comments made in the assessment results report. Once all assessment areas are compiled, the transit system is briefed on the outcome and provided the complete report. This data then gets compiled along with the other systems that have been assessed to produce overall national results in each Action Item category. This result leads to the analysis of weak and strong areas, not only of the individual systems, but also of the collective mass transit and passenger rail mode nationally. The results ensure program and grant funding priorities align with identified needs for security enhancement. TSA-assisted assessments are repeated approximately every 18-24 months to measure progress in the enhancement of security. The threat and consequences factor provided by DHS is a combined numeric score ranging from 1 to 6 with 6 representing the greatest threat and largest consequences. This factor is multiplied by the difference between a perfect score of 100 and the score the agency received in the BASE assessment to produce a system risk score. The aggregate of all the systems scores represent the total mass transit and passenger rail security risk. Comparing two annual aggregate scores will determine the percent reduction in transit security risk.

This data is reliable because TSIs use a common, standard checklist during the assessment process. TSA performs quality reviews on the assessment data that is collected and has completed enough assessments over time to be able to identify the types of inconsistencies that may arise and correct them when necessary. The threat and consequences factor, provided by DHS, is the same that the Division uses throughout the grant programs. Each factor is as reliable as the intelligence information and other data used in its determination.

The data is reported to the Division in a comprehensive report by the TSIs who actually conduct the assessment after briefing the mass transit or passenger rail agency on the results. The report is reviewed for quality by senior STSIP staff, and then made available to Division staff for review. These processes may result in inquiries to the appropriate inspectors for clarifying information. Ultimately, results are maintained for each assessed agency as well as consolidated into a national report of overall security posture in the Security and Emergency Management Action Items. Analysis for strengths and weaknesses, consistency or divergence from other agencies, trends, and smart practices occurs from these qualitative reviews.

To inform the immediate prioritization of security activities and resource allocations, the Division has adopted the Objectively Measured Risk Reduction methodology. This methodology, illustrated in figure C4-1, focuses on maximum immediate impact for the resources spent on risk reduction. Through this methodology, several objectives are achieved:

- Measurable baseline standards, or acceptable levels of risk exposure derived from best practices, are set and serve as a benchmark for security improvement to inform risk reduction activities;
- Current state of security in a transportation network is assessed through the BASE program described above, and compared to the risk reduction target;
- Security gaps are identified, expressed as the quantifiable difference between the desired state and the existing state, and prioritized;
- Measures and initiatives to close these gaps are identified and applied; and
- Risk reduction is measured through metrics which reflect a quantified level of baseline risk and the progress in risk reduction.

It is important to emphasize that these measures are developed with full consideration of transit security practitioners' requirements to ensure that they are realistic and practical for the industry.

Figure C4-1: Objectively Measured Risk Reduction



To close the prioritized gaps in mass transit and passenger rail systems identified through this methodology, TSA leverages randomness and unpredictability, smart application of technological tools, and coordinated training and outreach efforts to security partners.

5. Security Gaps and Mitigation Strategies

The following is a description of security gaps that continue to be addressed in each of the programs and processes listed in Security Programs and Processes Section of this document. This information is in part derived from the data generated using results of BASE reviews completed to date by the STSIP at TSA, and reflects the current implementation status of the Transit Security Fundamentals and the FTA/TSA Security and Emergency Management Action Items.

5.1 Information Sharing

There are two security gaps in information sharing:

- A minority of the top 100 transit agencies have yet to enroll in HSIN.
- The ability to disseminate such material to properly cleared transit agency officials in a timely manner.

Although the PT-HSIN portal 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 JTTF. All STSIP offices now possess portable secured telephones. If the need arises, TSIs can facilitate secure communications with chiefs of security for transit agencies through these telephones. Advances were made in these areas in 2009 with more systems on PT-HSIN and in possession of portable secure phones.

5.2 Employee Security Training

The BASE program findings continue to demonstrate that while many transit agencies provide initial antiterrorism 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 National Incident Management System (NIMS) and agency-developed incident command systems and incident response protocols to IEDs and Weapons of Mass Destruction, are being addressed through the development of a Mass Transit Security Training Program and the 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 who are in classes. TSA is committed to expedite processing to get funds to transit agencies. Mass Transit SCC and other industry representatives have indicated that the current funding does not support continuous necessary frontline employee training.

In addition to the training program described above, pursuant to sections 1408 and 1517 of the 9/11 Act, TSA is developing regulation requiring certain transit agencies and passenger railroads, to provide various security-related training to frontline employees.

5.3 Security Awareness Campaigns

While there is a lack of well-designed public awareness campaigns that employ innovative ways to engage and inform transit riders and employees about the threat from terrorists, there have been some significant efforts to augment the existing Transit Watch program. One of these efforts is a TSA transit employee poster program. Designed by TSA, these posters allow the individual agencies to adapt them to their specific environment by including their comments and pictures. This program has become popular and a similar one is being started for the transit riders as well. A new employee reminder card has been developed by TSA. On one side, the card deals with the subject of "What makes a package Suspicious," and the other side has the "7 Signs of Terrorism." These cards are being distributed to transit agency employees. During the summer of 2010, DHS rolled-out a national "If You See Something – Say Something" campaign to fill the void of well-designed public awareness programs. This program is the centerpiece of a joint effort by TSA and the National Transportation Security Centers of Excellence program under DHS S&T to augment this campaign's outreach in communities that have been the focus of significant transportation security outreach efforts in the past.

5.4 Research and Development and Technology Deployment

There is a capability gap associated with several transit system security vulnerabilities. For example, we have identified the need for conducting blast modeling for underwater tunnels and 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 explosives 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.

TSA also needs to expand the range of technology tools available for deployment in joint exercises with transit agencies under the VIPR program. Expanded regional availability of explosives trace detection equipment will augment the effectiveness of the joint security exercises. Methods and techniques to further enhance frontline employee training and awareness programs to improve system security have also been identified by industry representatives as an important area of research and development.

TSA and its Federal partners have consistently enjoyed the support of the industry and its representatives in this area. However, in an effort to ensure that research and development is responsive to industry requirements, TSA is committed to further engagement of its security partners in its efforts to identify practical technologies to improve system security. To that end, industry representatives participate as an integral component of the multi-agency Transportation Sector Research and Development Working Group whose primary mission is to improve coordination and prioritization of transportation research and development efforts and to leverage these programs across the stakeholder community.

5.5 Underwater/Underground Tunnels

TSA has identified a gap in underwater tunnel security. In response, TSA led the formation of an interagency Tunnel Risk Mitigation Working Group, bringing together subject matter experts from multiple Federal agencies. This team leveraged the capabilities of DHS S&T and other experts to conduct structural vulnerability assessments across all 29 underwater tunnels in the rail and transit community. The study showed that 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. As a result, TSA, as part of the TSGP, identified the protection of underwater tunnels as one of its priorities. Over the last few years, transit properties have invested millions of dollars in protecting these tunnels through both operational and hardening measures. Simultaneously, this group identified very specific research and development gaps that currently exist and is now addressing these gaps.

During this process, it also became evident that transit properties with underwater tunnels do not share information with each other on operational and hardening efforts underway to protect these tunnels. To mitigate this, TSA sponsored an Underwater Tunnel Security Information Forum in FY 2010. This forum brought together transit properties with underwater tunnels and provided them with an opportunity to discuss operational and tunnel hardening measures across the community. It also provided update on research and development activities at the national level to protect the Nation's underwater tunnels from an explosive event.

5.6 Drills and Exercises

At the time of the initial issuance of this plan, TSA found that a broader effort was 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 indicated that transit agencies were generally doing well in conducting drills and exercises, but more effort was needed in leveraging national exercises capabilities developed at DHS and adapting them for application to transit agencies in regional exercises. Facilitating this expanded effort through targeted grant funding for cross-functional, interagency regional exercises continues to be a strategic priority for TSA.

To meet this priority and enhance terrorism prevention and immediate response capabilities, TSA is developing a national exercise program. The initial effort has been in partnership with mass transit and passenger rail agencies in the National Capital Region. The objective is to produce a package for nationwide distribution to facilitate planning, preparation, and execution of a multi-phased, multi-jurisdictional, and cross-functional anti-terrorism exercise program. A few such exercises have been conducted across the country and TSA is incorporating the lessons learned from these exercises into the package. Topics for the exercises include vertical and horizontal flow of intelligence and information between agencies; internal capabilities and procedures used during periods of high threat; interactions with other transit and law enforcement agencies in the greater region; and sharing of best practices for transit emergency preparedness. Emergency scenarios range from suspicious activities to known terrorist threats.

The current organizational and funding construct for the Division imposes some significant challenges, namely in available funding. 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. TSA must, through a risk-based approach, maximize the security effectiveness of the resources available.

5.7 Cybersecurity

Transit and passenger rail systems rely on computerized networks to facilitate operations, enable communication, and enhance efficient service delivery. This makes them vulnerable to network failure and cyber attacks. Network failure may be caused by faulty or damaged internal components, direct cyber attack to the agency's network, an attack to a peripheral system or network, insider threat, unauthorized access to control center networks, or a blanket computer virus. The result may be loss of communications or operations capabilities as well as misinformation by hacking into a website or server.

The mass transit and passenger rail mode appears to be a popular target for cyber attacks. Several attacks have made national and international news over the past few years. Because of the significance of this threat, TSA has been working with its security partners to develop a comprehensive strategy to protect, defend, and respond to cyber attacks in the mode. The specific elements of the Mass Transit Cybersecurity program include:

Strategy Development—Underlying the current cybersecurity effort in the mass transit and passenger rail mode is a broad-scoped proactive approach being coordinated with the Transportation Systems Sector Cyber Working Group (TSS CWG) to put both a strategy in place that encompasses a security methodology that will identify risk and mitigating actions to this critical element, along with a plan to identify the implementation elements needed to ensure necessary inspections and information collection is conducted. As an adjunct to the current BASE program, TSA is in the process of linking those cyber elements and processes that are contained and used within the mass transit and passenger rail mode with the periodic BASE assessment process conducted by TSIs on the largest 100 mass transit and passenger rail agencies. This addition to the BASE program will allow for a smooth transition of the cyber element into the existing inspection programs, making it the 18th element that will be examined during routine and continuing TSIs-conducted assessments. TSA will also be participating in the newly formed APTA Cyber Security Standards Development Working Group, which aims to develop standards and recommended practices for transit and passenger rail agencies.

6. Way Forward

To achieve the objectives identified in this document and enhance security in mass transit and passenger rail, TSA has identified and is currently focusing on the following priorities. These priorities are the result of the collaborative efforts of government and industry partners under the GCC/SCC framework, discussed through CIPAC workshops, roundtables, and the PAG, and in conjunction with analysis of BASE program assessments of the 100 largest top transit systems.

- A risk-based approach will continue to be used to determine security priorities as they change.
- Complete development and implementation of a comprehensive risk assessment capability. Currently, the BASE program and/or TVC assessments are the foundation for identifying vulnerability gaps in transit agencies. As a new risk tool is implemented by TSIs, more weight will shift to the analysis of the results from the new tool.
- TSA's review of the BASE assessments for the 100 top transit agencies for 2009 shows that the national profile has not changed significantly from the previous year and the priorities for the average agency remain:
 - Training, operational deterrence, drills, and public awareness activities;
 - Multi-user high-density key infrastructure protection;
 - Single-user high-density key infrastructure protection;
 - Key operating asset protection; and
 - Other targeted risk mitigation activities.
- TSA continues to augment local anti-terrorism efforts with resources, such as Transportation Security Officers participating on mobile screening teams with Amtrak police to screen passengers and the New York Police Department in New York subways. TSA VIPR teams continue to work with local partners to support hundreds of annual operations. TSIs work with local operators to assess security status and help those stakeholders raise their security posture. The goal is to expand these efforts to additional high threat urban areas.
- TSA relies on a multi-faceted approach to protect assets and systems whose targeting by terrorists threatens the most extensive potential consequences. One of TSA's top priorities is hardening and protective actions for underwater tunnels, bridges, and multi-user, high-volume stations.
- Long-term strategic plans for mass transit and passenger rail security will address issues identified in TVC assessments and BASE results.
- Long-term strategies often require long-term projects to implement large and complex risk mitigation programs. The planning approach should include both design and implementation phases. Long-term projects will be considered for Federal assistance, recognizing that it may require support over multiple years to complete the project. Federal support, once begun,

will be available over the number of years identified until the project is complete in order to allow that program to be implemented.

- Some mass transit and passenger rail agencies lack a dedicated security or police force. A security priority is to make Federal assistance available to provide security liaison teams in local law enforcement departments in the operating areas of these agencies.
- While most of the security priorities are rightfully focused on the mass transit or passenger rail agency, there is concern about the ability of these agencies to communicate with security, law enforcement, and emergency management partners within their regions during threats or incidents. Regional interoperable communications and data systems are security priorities for mass transit and passenger rail systems.
- Finally, there will be a comprehensive and coordinated effort to develop and implement a cyber security strategy that will be incorporated within the framework of the BASE assessment program. This will allow for periodic risk assessments on the largest 100 transit agencies by TSIs. This comprehensive approach will involve TSA providing support for training opportunities to transit employees; funding to support pilot program testing procedures on different size and scope transit and passenger rail agencies; partnering with transit agencies, national laboratories, and associations in order to glean the best practices and procedures that will enhance overall cybersecurity; and some red team exercising to ensure proper procedures are being followed by transit field personnel. TSA will also participate with associations and others to identify existing standards and best practices and to develop new ones where there are gaps.

TSA will continue to work cooperatively with the Mass Transit SCC and transit police/security practitioners regarding any actions or measures to enhance system security prior to proposed final development and implementation.

Annex D: Highway Infrastructure and Motor Carrier



Contents

1. Executive Summary	249
2. Introduction	251
3. Overview of Mode	253
3.1. Overview	253
3.2. Assets, Systems, and Networks	254
3.2.1 Highway Infrastructure Assets, Systems, and Networks	254
3.2.2 Motorcoach Assets, Systems, and Networks	255
3.2.3 School Transportation Assets, Systems, and Networks	255
3.2.4 Trucking Assets, Systems, and Networks	256
3.2.5 Multi- and Cross-Modal Assets, Systems, and Networks	256
3.3 Risk Profile	257
3.4.1 Federal Government Partners	257
3.4.2 State, Local, and Tribal Government Partners	258
3.4.3 Industry Partners	258
3.5 Information Sharing Mechanisms	259
3.5.1 Federal, State, Local, and Tribal Information Sharing	259
3.5.2 Private Industry Information Sharing	259
3.5.3 Information Sharing and Communication Mechanisms	260
4. HMC Strategy	261
4.1 Goals and Objectives	261
4.2 Risk Framework	262
4.3 Decisionmaking Factors	263
4.4 Risk Mitigation Activities	264
4.4.1 Infrastructure	264
4.4.2 Motorcoach	265
4.4.3 School Transportation	265
4.4.4 Trucking	265
4.4.5 Multi-/Cross-Modal	266
4.4.6 International Initiatives	267
4.5 Performance Metrics	267

5. Security Gaps	269
5.1 Security Plans	269
5.2 Security Assessments and Methodologies	269
5.3 Security Training	269
5.4 Security Exercises	270
5.5 Information Sharing and Communications	270
6. Way Forward	271
6.1 Security Planning	271
6.2 Security Assessments	271
6.3 Security Training	272
6.4 Security Exercises	272
6.5 Information Sharing and Communications	272
Appendix 1: Strategy for a National Highway Bridge Security Program	273
 List of Figures	
Figure D3-1: Ownership of U.S. Highways and Bridges	253

1. Executive Summary

This Highway Infrastructure and Motor Carrier (HMC) Modal Annex is one of six modal annexes to the Transportation Systems SSP, which is required by the National Infrastructure Protection Plan (NIPP). This annex to the SSP contains information on the current status and future plans of the HMC mode for the three-year planning cycle.

This annex describes the components that comprise the highway transportation system, what is currently being accomplished, and the goals and way forward for reducing risk and enhancing security across the mode.

Section 2 describes the collaborative approach to drafting the HMC Modal Annex. Section 3 provides an overview of the HMC mode and of the various components (i.e., assets, systems, and networks) that comprise the highway transportation system. This section also introduces the mode's risk profile, as well as its public and private partners. Section 3 concludes by commenting on the information sharing and communication mechanisms used within the HMC mode.

Section 4 specifies the sector's strategy, including its goals and objectives, risk framework, and the decisionmaking factors that impact protection and resiliency policy. This section also reports on several of the processes, tools, programs, and initiatives aimed at mitigating modal risks. Section 4 concludes with a discussion of performance metrics for these risk mitigation activities.

Section 5 presents some of the security gaps that require the sector's attention. Section 6 addresses programs relevant to the sector to help attain the overall modal goals and objectives for closing the security gaps depicted in section 5, including several efforts that are presently underway.

In 2008, TSA completed work on the attached "National Strategy for Highway Bridge Security," a brief but comprehensive three-phase approach for identifying and assessing vulnerabilities of the Nation's most critical highway structures. Working with other agencies within DHS and DOT, the strategy is designed to eliminate overlap in Federal security reviews; speed available assistance to state, local, and municipal operators of important structures; and advocate future security considerations during the design of new and significantly renovated highway structures. The strategy is currently due for biennial review by the panel of agencies that created the original document.



2. Introduction

The HMC Modal Annex to the Transportation Systems SSP is a joint effort between the Highway and Motor Carrier Government Coordinating Council (GCC) and the Highway and Motor Carrier Sector Coordinating Council (SCC). The GCC partnered with Federal, State, local, and tribal stakeholders in drafting this annex. The SCC, consisting of owners and operators and associations from the trucking, motorcoach, school transportation, physical infrastructure, and related industries, met with the GCC as part of a Joint Working Group and Writing Team to further develop and draft this document. It defines goals and objectives of the mode and presents a strategic plan to achieve the protection of the highway transportation system, mitigate vulnerabilities, and improve response capabilities for a transportation security incident or other all-hazards event.

The system's assets include, but are not limited to, bridges, major tunnels, operations and management centers, trucks carrying hazardous materials (HAZMAT), other commercial freight vehicles, motorcoaches, school buses, and key intermodal facilities. While the in-vehicle facilities and highway infrastructure facilitate the movement of people, services, and cargo is robust, some elements are critical to the maintenance of public health, economic vitality, telecommunications, electricity, and other essential services. The temporary debilitation of a bridge or tunnel could result in regional shutdowns, diversions, or costly repairs with potentially severe results.

Incidents and events include, but are not limited to, terrorist use of transportation system assets to attack critical infrastructure, direct targeting of the transportation system by terrorists, breaches of cybersecurity, and pandemic and natural disasters.

Vehicles that use the highways are potential targets or weapons that terrorists could use to attack critical infrastructure or other assets. The trucking industry is unique in that it is the only segment of the highway mode with complete intermodal supply chain relationships with aviation, maritime, mass transit, freight rail, and pipeline. The bus industry, similar to the trucking component, also operates with multi-modal interconnectivity daily, providing passenger and limited freight service on a national level. The diversity of these industries poses additional challenges to the effective integration of security into both large, complex operations and smaller owner-operator businesses.

Measures to secure the assets of the highway transportation system must be implemented in a way that balances cost, efficiency, and preservation of commerce. To address these security issues it is important that the Federal Government continues to work effectively within the established government/industry partnership, implementing a variety of security programs to enhance the security of domestic highway operations. Highway and Motor Carrier security is advanced by implementing layered security measures into transportation systems operations and management.

Toward this end, DHS, DOT, and private sector security partners continue to be committed to improving the highway transportation system. Technology and security awareness and expertise must keep pace with the increasingly sophisticated terrorist or criminal techniques that may be used to threaten the highway transportation system or its components. The HMC Modal Annex may require a periodic update to reflect current conditions, enhanced strategies, new programs, and GCC/SCC scope of planning. Federal, State, local, territorial, and tribal government agencies, along with private stakeholders, collaborate in the national effort to maintain the capability to move freely and facilitate interstate commerce.

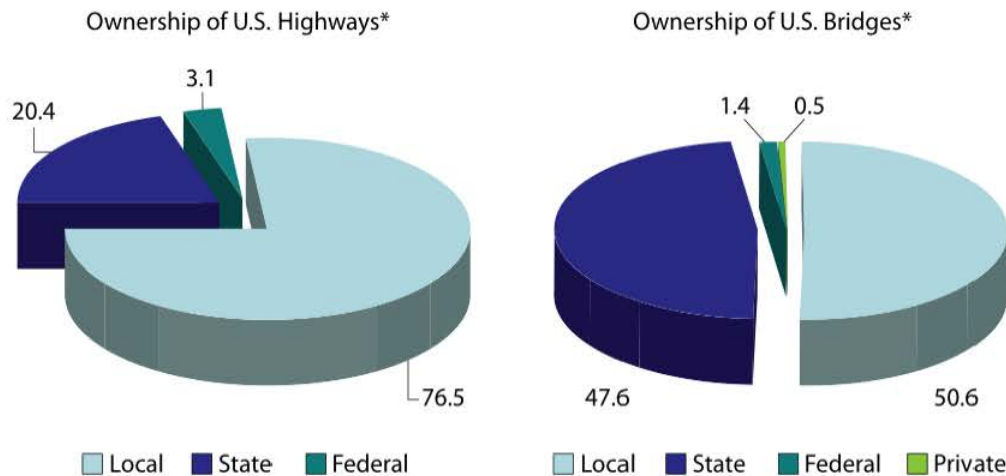


3. Overview of Mode

3.1 Overview

Highways, bridges, and tunnels are crucial components of the public infrastructure of the United States and form the backbone of America’s transportation network, in that all modes rely on highway infrastructure. According to the Federal Highway Administration (FHWA) Freight Analysis Framework Statistics, the Nation’s highway network includes nearly 4 million miles of roadway, almost 600,000 bridges, and some 400 tunnels in 35 states.¹ The network of highways, bridges, and tunnels connect all regions and States to almost every major piece of critical infrastructure, national landmark, multi-modal transportation infrastructure, and tourist destination, as well as to one another. Transporting people and goods across this network is critical for meeting the everyday needs of American citizens and businesses.

Figure D3-1: Ownership of U.S. Highways and Bridges



The Federal government has played a key role in shaping the highway network, by regulating interstate commerce and by funding and facilitating transportation improvements, while balancing diverse needs and interests. Since the attacks of September 11, 2001, the Federal government exercised greater authority over the security of the Nation’s highway network and

¹ DOT provides this data through its Bureau of Transportation Statistics and through the FHWA.

protection of its critical infrastructure. State and local governments and businesses, however, are essential partners with the Federal government in the development and operation of the Nation's highway network.

Although most of the transportation infrastructure in the United States is funded and maintained by the public sector, with the private sector playing a smaller but increasing role, it is local governments who own and operate more than 75 percent of the Nation's nearly 4 million miles of roadway and over half of its nearly 600,000 bridges.² Furthermore, most of the vehicles used on the Nation's transportation network are owned and operated by private individuals and firms. Thus, protecting the Nation's highway network is truly a shared responsibility between State and local transportation agencies, their sister agencies responsible for law enforcement, Federal transportation agencies, the private sector, and the public, all of whom travel over three billion vehicle highway miles annually.³

3.2 Assets, Systems, and Networks

3.2.1 Highway Infrastructure Assets, Systems, and Networks

The **National Highway System (NHS)** is comprised of approximately 160,000 miles of roadway important to the Nation's economy, defense, and mobility, including the Interstate Highway System. It was developed by DOT in cooperation with Department of Defense (DoD), the States, local officials, and Metropolitan Planning Organizations (MPOs). The NHS includes the following subsystems of roadways:⁴

Eisenhower Interstate Highway System of highways retains a separate identity within the NHS.

Other Principal Arterials in rural and urban areas provide access between an arterial and a major port, airport, public transportation facility, and/or other intermodal transportation facility.

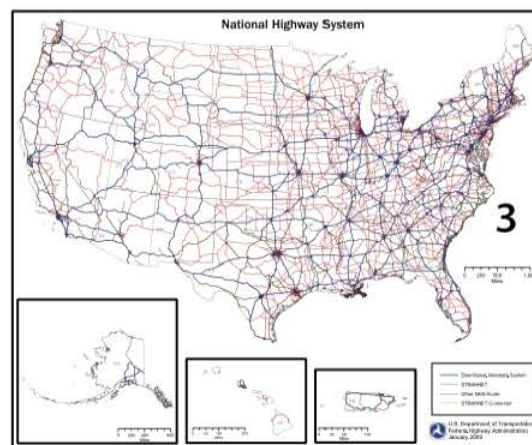
Strategic Highway Network (STRAHNET) is a network of highways which are important to the strategic defense policy of the United States and which provide defense access, continuity, and emergency capabilities for defense purposes.

Major Strategic Highway Network Connectors are highways that provide access between major military installations and highways that are part of the STRAHNET.

Intermodal Connectors are highways that provide access between major intermodal facilities and the other four subsystems making up the NHS.

Other Assets

Message signs, both fixed and portable, are referred to by a variety of names. Electronic traffic signs are used on roadways to give travelers information about special events and occurrences that disrupt the normal flow of traffic, such as accidents,



² U.S. Department of Transportation's Report to Congress - 2006 Status of the Nation's Highway, Bridge, and Transit: Conditions and Performance, <http://www.fhwa.dot.gov/policy/2006cpr/index.htm>.

³ Ibid.

⁴ A specific highway route may be on more than one subsystem.

roadwork, and disabled vehicles. AMBER Alerts and warnings and alerts about other types of criminal, terrorist, or suspicious activity, are also relayed over the mode's network of message signs.

Traffic Management Centers (TMCs) are found primarily in large urban areas and are operated by local transportation agencies. They are usually 24/7 operations centers responsible for monitoring and controlling traffic in designated sectors and for coordinating transportation agency response to emergencies. Some states are forming regional centers, such as the Kansas-Missouri joint center near Kansas City, to manage traffic regionally. Many centers are now being co-located with other public safety, fire, and EMS responders. These centers are often referred to as traffic operations centers.

Publicly and privately owned and operated rest areas provide for highway user safety and convenience.

3.2.2 Motorcoach Assets, Systems, and Networks

The motorcoach industry is comprised of approximately 3,137 for-profit companies operating some 29,325 buses and employing over 118,000 people in full and part-time jobs. These companies operate primarily in interstate operations that include wholly-owned bus terminals, shared terminals with other transportation modes such as passenger rail, charter group determined pick-up and drop-off locations, or from their own company property. Motorcoaches carry approximately 751 million passengers annually to millions of destinations in the United States, Canada, and Mexico. Destinations may include attractions located in urban areas, national and State parks, and high volume tourist sites. For the most part, there are no industry-wide operations, cyber systems, or networks beyond the normal business systems used by individual passenger carriers for trip scheduling and financial operations; however, the National Bus Traffic Association's (NBTA) computers form a single network that acts as the monthly interline ticketing financial clearinghouse for approximately 70 intercity scheduled carriers. NBTA's computers are protected from cyber attacks through security measures and scheduled system backup by the computer service provider. Some additional specific motorcoach industry assets, systems, and networks are as follows:

- Not-for-profit private motorcoach operators such as churches and other non-profit groups or organizations;
- Motorcoach manufacturers;
- Sellers of new and used motorcoaches;
- Motorcoach industry component and service suppliers, such as insurers, repair facilities, and parts vendors;
- Motorcoach industry travel partners, comprised of destinations or attractions, such as resorts, hotels, casinos, and cruise lines throughout the Nation; and
- Cross-sector interdependencies such as chartered motorcoaches and cruise lines or school bus charters for special events.

3.2.3 School Transportation Assets, Systems, and Networks

The school transportation industry is a network that ensures the safe and secure transportation of 23 million students to approximately 80,000 different schools within 15,000 school districts. The assets of this system include 460,000 school buses, approximately 15,000 parking and maintenance locations, and more than 500,000 drivers, maintenance personnel, and staff officials. For the most part, each school district is an independent entity working within the boundaries of State and Federal rules and statutes. This independence is especially evident in the local relationships with law enforcement and first responder agencies. Approximately 70 percent of school transportation assets are owned and operated by the individual school districts, and approximately 30 percent of school transportation assets are privately owned by for-profit companies and are contracted for use by the districts, including the drivers.

3.2.4 Trucking Assets, Systems, and Networks

While some carriers have large, integrated, national networks, the industry as a whole is highly fragmented. According to DOT registrations, there are more than 214,000 for-hire motor carriers and an additional 27,600 private trucking fleets operating in interstate commerce. Additionally, there are 89,000 other DOT-registered trucking fleets, including some that operate only in intrastate commerce. These fleets operate over 29 million trucks, hauling more than 10 billion tons of freight annually. Among motor carriers, 96 percent operate 20 trucks or less, while 87 percent operate 6 trucks or less. The trucking industry employs 8.9 million people, of whom nearly 3.5 million are drivers.⁵

Canada and Mexico are the United States' largest and third largest trading partners, respectively. In 2007, trucks hauled 58 percent of goods between the United States and Canada (\$325 billion) and 66 percent between the United States and Mexico (\$230 billion). As the North American economies become more integrated, trucking's importance in international trade should grow. Nearly every good consumed in the United States is put on a truck at some point. The industry hauls 69 percent of all freight in the United States, by weight, and 83 percent of all freight by value.

Most operational systems and networks are held by individual companies. However, some programs, such as the TSA-sponsored Highway Information Sharing and Analysis Center (ISAC), do act as information sharing networks. Other trucking assets, systems, and networks include the following:

- Truck manufacturers
- Truck and vehicle rental leasing companies (and their associated cyber networks)
- DoD's Surface Deployment and Distribution Command
- General Services Administration/FEMA contracting networks
- Customs & Border Protection's Automated Commercial Environment/Truck eManifest System

3.2.5 Multi- and Cross-Modal Assets, Systems, and Networks

The HMC mode connects other transportation system sector assets and infrastructures. The motorcoach and trucking industries intersect with multiple modes of transportation, as well as the other 17 CIKR sectors. Additional multi- or cross-modal assets, systems, and networks include the following:

- Intermodal cargo facilities (with the rail, aviation, and maritime modes);
- Commercial drivers schools;
- State drivers licensing systems and networks;
- State vehicle registration systems and networks;
- Vehicle insurance carriers;
- Transportation business insurance carriers; and
- Truck stop owners and operators.

⁵ U.S. Department of Transportation's Report to Congress - 2006 Status of the Nation's Highway, Bridge, and Transit: Conditions and Performance, <http://www.fhwa.dot.gov/policy/2006cpr/index.htm>.

3.3 Risk Profile

The HMC mode's security risks are evidenced by attacks either using or against the mode, including the 1993 attack against the World Trade Center in New York, the 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City, and more recent illustrations in Iraq and Afghanistan of improvised explosive devices placed on or near highway infrastructure, vehicle-borne improvised explosive devices, and attempts to use tankers with hazardous materials in truck bombings. There are also documented plots against various components of highway infrastructure, such as the Brooklyn Bridge. These examples are a sobering reminder that the highway system remains an attractive target for terrorists.

Hurricanes, earthquakes, forest fires, and other disasters (natural and industrial) also highlight risks to the HMC mode that are not directly related to terrorism. Risks from both terrorist attacks and other hazards demand a coordinated approach involving all stakeholders. In the wake of the attacks of September 11, 2001, the HMC mode joined together in an unprecedented way to protect its customers, systems, and assets. Private industry continues to make contributions to sector-wide risk mitigation efforts. State and local governments have enhanced first-response capabilities, increased vigilance, and secured potential targets. Cooperation among its diverse stakeholders is one of the strengths of the HMC mode.

3.4. Partners and Relationships of Highway and Motor Carrier Mode

3.4.1 Federal Government Partners

The objective of the Highway GCC is to coordinate highway and motor carrier protection strategies and activities; to establish policies, guidelines, and standards; and to develop program metrics and performance criteria for the mode. The Highway GCC fosters communication across the government and between the government and private industry in support of the Nation's homeland security mission.

The Highway GCC, whose membership consists of key Federal departments and agencies responsible for or involved in highway and motor carrier protection, recognizes the integral relationship that it has with similar GCCs for other modes and will leverage its participation with these other councils to connect issues across modes at appropriate levels of government and with private industry. The Highway GCC will add permanent Federal government or agency members, as deemed necessary and appropriate. The Highway GCC will extend invitations to *ad hoc* members with special expertise from other departments, agencies, or offices from time to time to meet expertise requirements necessary to fulfill its mission. In addition, the membership may be expanded to include State/local officials and organizations with an interest in the HMC mode.

Member organizations of the Highway GCC include:

- Transportation Security Administration;
- Federal Motor Carrier Safety Administration;
- Federal Highway Administration;
- National Highway Traffic Safety Administration;
- Pipeline and Hazardous Materials Safety Administration;
- Department of Defense;
- Department of Education;
- Department of Energy;
- General Services Administration;
- Nuclear Regulatory Commission;

- DHS Customs and Border Protection;
- DHS Office of Infrastructure Protection;
- DHS Homeland Infrastructure Threat and Risk Analysis Center;
- DHS Federal Emergency Management Administration;
- DHS Office for Intergovernmental Affairs;
- Federal Bureau of Investigation;
- United States Department of Agriculture, Food Safety, and Inspection Service;
- American Association of State Highway Transportation Officials;
- Commercial Vehicle Safety Alliance;
- American Association of Motor Vehicle Administrators;
- International Association of Chiefs of Police;
- National Sheriffs' Association; and
- National Association of State Directors of Pupil Transportation Services.

3.4.2 State, Local, and Tribal Government Partners

State, local, and tribal governments manage protection efforts for the highway sector assets, systems, and networks within their jurisdiction. They serve as crucial coordination hubs, bringing together prevention, protection, response, and recovery authorities, capabilities, and resources of the various jurisdictions. State, local, and tribal agencies are often the first on the scene of a transportation security incident, whether it is a natural or manmade incident. Federal agencies work closely with these partners to coordinate protection efforts and collaborate with the owners or operators of the Nation's transportation infrastructure.

3.4.3 Industry Partners

The private industry-led Highway SCC is a counterpart to the Highway GCC. Working in partnership, the Highway GCC and SCC collaborate to review and develop security programs necessary to protect the Nation's highway and motor carrier mode.

The following are member organizations of the Highway SCC:

- American Bus Association;
- American Chemistry Council;
- American Petroleum Institute;
- American Road and Transportation Builders Association;
- American Trucking Association;
- Border Trade Alliance;
- Chemtron;
- Con-Way, Inc.;
- Detroit-Windsor Truck Ferry;
- Institute of Makers of Explosives;
- Intelligent Transportation Society of America;

- Intermodal Association of North America;
- International Bridge Tunnel and Turnpike Association;
- Kenan Advantage Group;
- Laidlaw Education Services;
- Mid-States Express, Inc.;
- National Association of Small Trucking;
- National Association of Truck Stop Operators;
- National Industrial Transportation League;
- National School Transportation Association;
- National Tank Truck Carriers, Inc.;
- Owner-Operator Independent Drivers Association;
- Schneider National, Inc.;
- Seaton & Husk, L.P.;
- Taxicab, Limousine and Paratransit Association;
- The BusBank;
- The National Academies, Transportation Research Board;
- Tri-State Motor Transit Company;
- Truck Manufacturers Association;
- Truck Rental and Leasing Association; and
- United Motorcoach Association.

3.5 Information Sharing Mechanisms

3.5.1 Federal, State, Local, and Tribal Information Sharing

The establishment of the SCC and GCC under the Critical Infrastructure Protection Advisory Committee (CIPAC), and other coordinating bodies, such as the Critical Infrastructure Cross-Sector Council and ISACs, has greatly improved information sharing among stakeholders. Information sharing previously relied upon personal relationships among Federal, State, local, and HMC owners/operators. These relationships may have been well-established and effective, but unfortunately, many other critical stakeholders were left without access to essential information.

In addition, recent efforts to improve the Homeland Security Information Network (HSIN) have resulted in a better information-sharing system. While this system still needs to mature, it significantly improves upon the initial information-sharing mechanism.

3.5.2 Private Industry Information Sharing

HMC industry owners/operators have primary responsibility for protection of the mode's infrastructure. Overall, information sharing and analysis processes would benefit by using industry expertise to analyze and disseminate information and help identify what is important for the entire sector or a specific mode.

3.5.3 Information Sharing and Communication Mechanisms

Communication between public and private stakeholders in the HMC mode happens through several methods, such as direct mail, broadcast e-mails, public websites, secure DHS portals, teleconferences, GCC/SCC CIPAC quarterly meetings and Intermodal Security Training and Exercise Program (I-STEP) workshops or exercises. TSA uses many of these methods to promote and distribute its brochures, tip cards, posters, and educational security awareness materials. TSA shares information that has an actionable aspect, such as an incident reports, security bulletins, or alerts with private stakeholders through the following mechanisms:

- **Incident-related information sharing.** The First Observer® program operates the Highway ISAC. First Observer® has received funding through the Trucking Security Program (TSP), a Federal security grant program. Additionally, TSA operates the TS-ISAC through the HSIN communications network.
- **Homeland Security Information Network-Critical Sectors.** HSIN-CS is a secure, single-source, information-sharing, web-based network to assist in the two-way communication of infrastructure protection-related information. HSIN-CS plays a key role in supporting the ongoing operations and resiliency of the Nation's critical infrastructure by creating an online community for a vetted group of critical infrastructure stakeholders to communicate within the group as well as with DHS. This role will likely strengthen as the number of people using the network increases and a more robust information-sharing environment evolves over time.

Within HSIN-CS, a portal (HSIN-CS/HMC) has been created to provide HMC focused materials and communications. This portal allows for different user groups such as Trucking, Motorcoach, GCC, and the SCC to have secure areas to conduct more in-depth and specific information sharing and work collaboration areas that are specific to their individual needs. Access to the portal and sub-portals is granted through established protocols agreed to by the mode's CIPAC partners.

- **Alerts, warnings, and notifications.** TSA operates an emergency notification system, the TSA Alerts system. A Federal grant funds the Highway ISAC operated by the First Observer® program. This ISAC disseminates information bulletins, alerts, and other security-related reports to stakeholders via email. It also works with both public and private stakeholders to collect, share, and analyze information that increases the security of the mode. Private sector partners also report suspicious activity that could signal pre-operational terrorist activity to the DHS National Operations Center (NOC) through the National Infrastructure Coordinating Center (NICC).
- **5-1-1 Traveler Information System,** deployed in 45 states, is a transportation and traffic information telephone hotline available to landline and mobile phone users. It can be used to provide weather, traffic conditions, and other information deemed of value to highway users.
- **Regional coalitions** are formed to improve information sharing and collaboration along lengths of highways that traverse more than one state. These coalitions are valuable in coordinating messages during events that impact traffic regionally or for distributing a consistent message as travelers are passing through states. An example is the I-95 coalition, comprised of states along the eastern seaboard through which I-95 passes. The coalition ensures all states are displaying the same information on message signs relative to incidents or events along the congested east coast corridor.

4. HMC Strategy

4.1 Goals and Objectives

The mission of the Transportation Systems Sector is to continuously improve the risk posture of the national transportation system. The SSP identifies a number of goals for enhancing security from disruptive incidents. The HMC mode shares these goals and defines objectives consistent with and particular to the mode. These goals set the stage not only for what is being addressed by Risk Mitigation Activities (RMAs) described in Section 4.4 but also in determining the future areas to be addressed as described in section 6.

Goal 1: Prevent and deter acts of terrorism using or against the highway transportation system.

Objectives

- Implement risk management-based flexible, layered, and measurably effective security programs.
- Increase vigilance and awareness of highway travelers and HMC workers.
- Ensure that security policies and practices recognize and facilitate the legitimate movement of goods and people.
- Develop processes that identify critical cyber infrastructure and implement measures that address strategic cybersecurity priorities.
- Enhance cross-modal and cross-sector coordination mechanisms to address critical interdependencies.
- Strengthen coordination within the private sector and between the public and private sectors.

Goal 2: Enhance the all-hazard preparedness and resilience of the highway transportation system to safeguard U.S. national interests.

Objectives

- Develop risk-based strategies to strengthen and provide increased resilience of highway systems, networks, and assets.
- Enhance the capacity and capability of the response community for rapid and flexible response to, and of private sector HMC partners to recover from, terrorist attacks and other all-hazard incidents.
- Evaluate and take actions to reduce the impact of critical surges affecting the highway transportation system during emergency situations in high threat urban areas.
- Strengthen coordination within the private sector and between the public and private sectors.

Goal 3: Improve the effective use of resources for highway transportation security.

Objectives

- Coordinate policy and eliminate duplication of efforts by Federal, State, and local government agencies.
- Recognize the progress and success the HMC mode has made to address highway transportation security needs.
- Use risk and economic analyses as decision criteria to align sector resources with the highest priority HMC security risks.
- Enhance HMC participation in the development and implementation of public sector highway system security programs as needed.
- Ensure coordination with HMC industry partners in the risk-based selection and prioritization of Transportation Systems Sector security research, development, test, and evaluation (RDT&E) efforts.
- Strengthen coordination within the private sector and between the public and private sectors.

Goal 4: Improve highway situational awareness, understanding, and collaboration.

Objectives

- Enhance information and intelligence sharing among HMC modal partners.
- Educate public and private partners on resiliency and risk management best practices within the highway mode.
- Assess, manage, and share situational awareness of international highway security and resiliency interdependencies.
- Strengthen coordination within the private sector and between the public and private sectors.

4.2 Risk Framework

The diversity of the HMC mode necessitates a variety of initiatives and methods to evaluate and mitigate the risk environment. Like its other counterparts within the sector, the HMC mode faces a dynamic risk environment categorized by risk to the mode and risk from the mode. It is therefore important to consider not only the protection of people, cargo, assets, and infrastructure, but also the potential use of elements of the mode for acts of terrorism.

While there are multiple definitions for risk, DHS describes risk as a function of threat, vulnerability, and consequence:

$$\text{Risk} = f(\text{Threat, Vulnerability, Consequence})$$

Threat, vulnerability, and consequence are therefore at the center of the mode's risk management efforts; each requires a different perspective and set of initiatives.

Threat Assessments

Obtaining, synthesizing, analyzing, and distributing relevant and credible intelligence information is essential to informing the mode's decisionmaking processes. When the SSA receives threat information it must be analyzed, filtered, and disseminated to modal partners, as classification and threat levels warrant, in a manner that improves awareness and, when necessary, generates appropriate action.

Vulnerability Assessments

Vulnerabilities of an asset, system, or network are the physical, human, cyber, or operational attributes that render it open to exploitation or susceptible to hazards. Vulnerabilities are weaknesses that, if exploited or compromised, diminish preparedness to deter, prevent, mitigate, respond to, or recover from one or more hazard scenarios. An assessment should describe the vulnerability in sufficient detail to assist in subsequent development of countermeasures and to facilitate risk reduction.

Consequence Assessments

Consequence assessment is the process of identifying and evaluating the potential or actual effects of an event or incident. Assessments occur throughout the mode, both informally and formally. The diversity of the HMC modes necessitates varied consequence assessments, which focus upon people, cargo, conveyances, and infrastructure.

Cross-modal Analyses and the HMC Mode

Cross-modal risk assessments may vary widely in scope and size, depending on mission focus (e.g., security or all hazards) and the situation. These analyses help identify strategic planning priorities and define long-term visions. Cross-modal analyses inform key leadership decisions, including investments in countermeasures.

The HMC mode shares responsibility for helping to enhance risk management efforts across the other modes constituting the Transportation Systems Sector. As such, the mode engages in sector-wide initiatives such as the Transportation Sector Security Risk Analysis (TSSRA).

TSA's Highway and Motor Carrier Division is currently preparing focused risk assessments of the following highway sub-modes: School Transportation, Trucking (including HAZMAT Trucking), Motorcoach, Highway Infrastructure, Port Interface, and Food Transportation by Commercial Trucking.

4.3 Decisionmaking Factors

With the range of information provided by the various risk assessments, as described above, the priorities of the HMC mode are subject to a variety of other influences and mandates. Budgetary limitations throughout the mode may constrain risk management decisions. Other factors, such as time constraints, the feasibility of countermeasures, and the protection of commerce and civil liberties, must also be considered. Below are the requirements from legislative and executive branches that shape the decisionmaking environment.

Congressional Requirements⁶

- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act)
- Aviation and Transportation Security Act of 2001 (ATSA)
- Maritime Transportation Security Act of 2002 (MTSA)
- Homeland Security Act of 2002 (HSA)
- Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)
- Implementing Recommendations of the 9-11 Commission Act of 2007, P.L. 110-53 (9/11 Act)

⁶ See Sector-Specific Plan Appendix 3: Transportation Systems Sector Authorities.

Executive Branch Requirements

- Homeland Security Presidential Directives (HSPDs)
- White House Executive Orders

Private Sector Input

The private sector may have concerns that relate to their business interests or based on knowledge of public interest, especially in the areas of safety or privacy. Awareness of these concerns helps to shape objectives and priorities.

4.4 Risk Mitigation Activities

TSA and its partners have developed numerous processes, tools, programs, and initiatives to reduce risk within the HMC mode. The following provides a summary of the risk mitigation activities (RMAs) for the modal elements of infrastructure, motorcoach, school transportation, trucking, multi- and cross-modal, and international initiatives. Each modal element will be discussed in relation to how it is meeting some, or all, of the goals listed in section 4.1.

4.4.1 Infrastructure

The RMAs that specifically seek to reduce infrastructure risks meet at least one of the objectives of each of the four SSP goals. The FHWA maintains a number of these infrastructure RMAs. Its Highway Infrastructure Protection and Emergency Management Professional Capacity Building website⁷ provides information and tools to highway or transportation agency employees desiring knowledge of highway infrastructure security and emergency management training, publications, or State contacts. The site is aimed at those newly assigned to positions in these functions, while current employees can benefit through the site's educational and research resources. Practitioners should find the site useful as a reference repository.

FHWA's First Responder Awareness to Terrorist Threats for Bridges and Tunnels workshop series gives first responders, such as law enforcement personnel, inspectors, and other emergency responders, an overall awareness of terrorist threats and structural vulnerabilities. More specifically, they learn to identify strengths and weaknesses of bridge and tunnel components and the damage to be expected for terrorist threats. Threats covered include vehicle-borne improvised explosive devices (VBIED), hand-emplaced improvised explosive devices (HEIED), non-explosive cutting devices (NECD), and fire and vehicle impact. Similarly, FHWA's Blast Design & Analysis for Bridge Structures workshop focused on the fundamentals of explosion effects, determining blast loads on bridge structures, computing structural response to blast loads, and the design and retrofit of structures to resist blast effects. The emphasis is on terrorist threats, including the VBIED and HEIED.

FHWA developed the Component Level Risk Management Methodology, which is designed to provide engineers and managers the capability to develop a cost-effective risk management plan for a structure using a component-level analysis. This is accomplished by identifying strengths and weaknesses of bridge and tunnel components, the damage to be expected from terrorist acts, and analysis of the risk of each component to a specific threat. Threats covered include the VBIED, HEIED, NECD, fire, and vehicle impact.

FHWA also developed an online course in Freight Security Awareness Training, which provides targeted training to build the knowledge base and skills of freight transportation and planning professionals.

The American Association of State and Highway Transportation Officials (AASHTO) developed the Costing Asset Protection: A Guide for Transportation Agencies (CAPTA), which is a tool that is used by transportation agencies to help manage and reduce risk. CAPTA provides a methodology for informing decisions by analyzing assets, relevant threats and hazards, and

⁷ <http://www.fhwa.dot.gov/security/emergencymgmt/profcapacitybldg/>.

consequence levels of interest. It provides the capability to iteratively evaluate threats and hazards against countermeasures and the costs involved.

4.4.2 Motorcoach

TSA manages three initiatives aimed at reducing risks for the motorcoach industry, which address two of the sector goals. TSA's Operation Secure Transport (OST) is a computer-based interactive training resource that is available to industry employees. Employees who complete the OST training learn how to recognize security threats, as well as how to respond to security incidents. The Intercity Bus Security Grant Program (IBSGP) through its distribution of grants to eligible stakeholders, creates a sustainable plan for protecting intercity bus systems and the traveling public from terrorism, especially from explosives and non-conventional threats that would cause major loss of life and severe disruption. For the fiscal year (FY) 2009, IBSGP awarded \$11.5 million. The TSA Highway and Motor Carrier Division provides subject matter expertise for evaluating grant applications.

4.4.3 School Transportation

There are two RMAs specifically aimed at reducing school transportation risks, which, combined, meet at least one of the objectives of each of the four sector goals. TSA's School Transportation Security Awareness (STSA) is a video training tool providing scenario-based situational awareness for school bus drivers and other industry personnel. The National School Transportation Association worked with the school transportation industry and TSA to create a voluntary list of security action items for school transportation industry administrators and employees.

4.4.4 Trucking

All of the RMAs specifically aimed at reducing risks to the trucking mode meet at least one of the objectives of each of the four sector goals.

There is considerable collaboration regarding the security of HAZMAT among Federal agencies, including DOT's Federal Motor Carrier Safety Administration (FMCSA), DOT's Pipeline Hazardous Materials Safety Administration (PHMSA), and TSA. Furthermore, these agencies collaborate with private industry. Congress directed FMCSA to establish the Hazardous Materials Safety Permit Program to produce a safe and secure environment to transport HAZMAT. Codified within PHMSA's regulations and rules, HM-232⁸ requires persons who offer for transportation or transport covered HAZMAT to develop, implement, and maintain security plans, as well as provide in-depth, employee security training. Motor carrier security plans must include an assessment of the possible transportation security risks for shipments of covered HAZMAT and include the following elements: personnel security, facility security, and en route security. Mandatory HAZMAT employee training must provide an awareness of security risks associated with HAZMAT transportation and provide in-depth security training on the elements of the security plan and its implementation.

FMCSA audits HAZMAT motor carriers to evaluate their compliance with security plans and security training as mandated under HM-232. Under its Secure Contact Review (SCR) program, inspectors are given authority to write citations for a carrier's failure to properly comply with the requirements. SCRs are conducted on all HAZMAT motor carriers that transport placardable amounts of HAZMAT.

PHMSA conducts periodic compliance investigations on HAZMAT motor carriers and shippers to evaluate their adherence with security plans and security training as mandated under HM-232. Inspectors are given authority to write citations for a carrier's or shipper's failure to properly comply with the requirements.

⁸ Hazardous Materials Transportation Security Requirements (HM-232): Security Plans.

TSA offers voluntary training initiatives, such as the HAZMAT Self-Assessment Training Program and its HAZMAT Motor Carrier Security Training Program, to assist motor carriers that transport placarded amounts of HAZMAT in developing a plan to address security risks. The TSA Highway and Motor Carrier Division has completed extensive analysis on industry security best practices during the transport of high risk HAZMAT and suggested, through voluntary Security Action Items (SAIs), that these practices be standardized throughout the HAZMAT industry. Training is available online through the TSA public website.

The Trucking Security (Grant) Program (TSP), managed by TSA, was intended to enhance homeland security through increased vigilance and awareness on our Nation's highways. The TSP funds the First Observer.® program, which seeks to assist all professionals and operating entities throughout the entire highway sector in obtaining training on security awareness, reporting suspicious incidents, and information analysis. There are three components to this program: the Call Center, the Highway ISAC, and training modules.

Industry is doing its part to promote RMAs that reduce risks in the trucking mode. For example, the American Chemistry Council operates the Chemical Transportation Emergency Center (CHEMTREC), which serves as a round-the-clock resource for obtaining immediate emergency response information for accidental chemical releases. CHEMTREC is linked to the largest network of chemical and hazardous material experts in the world including chemical and response specialists within the American Chemistry Council membership, response specialists within the carrier community, public emergency services, and private contractors. The Agricultural and Food Transporters Conference prepared a security guide titled, *Guide for Security Practices in Transporting Agricultural and Food Commodities* and a threat assessment tool document, *Resources Directory for Security Practices in the Transportation of Agricultural & Food Commodities*. These documents serve as a threat assessment tool and security planning guide for any trucking company that transports agriculture commodities.

4.4.5 Multi-/Cross-Modal

There are unique transportation security issues found in the multi- and cross-modal environment of the Nation's transportation security network. The RMAs specifically aimed at reducing risk in the multi- and cross-modal environment mode meet at least one of the objectives of each of the four sector goals.

TSA's I-STEP enhances the preparedness of our Nation's surface transportation sector network with meaningful evaluations of prevention, preparedness, and response to terrorist-related incidents. I-STEP improves security and resiliency capabilities by increasing awareness, improving processes, creating partnerships, and delivering transportation sector network intermodal security training and exercises.

TSA's Transportation Worker Identification Credential (TWIC) establishes a system-wide common credential used for all personnel requiring unescorted physical and/or digital logic access to secure areas of the maritime port systems. Background checks and biometrics are required to obtain a TWIC card.

TSA's Air Cargo Security Rule requires additional security measures throughout the air cargo supply chain, including performing security threat assessments on individuals with unescorted access to cargo, enhancing existing security and training requirements for indirect air carriers, and strengthening the Known Shipper Program. Motor carriers who transport unescorted cargo for indirect air carriers must undergo a security threat assessment and receive annual TSA-approved security training.

TSA has established several voluntary initiatives to assist industry stakeholders to improve security for their specific mode. For example, TSA's Certified Cargo Screening Program (CCSP) is a voluntary program designed to enable vetted, validated, and certified supply chain facilities to screen air cargo prior to delivering the cargo to the air carrier. The CCSP will create additional screening capacity and provide a practical, effective opportunity for screening to occur on individual pieces of cargo prior to consolidation. TSA also uses SAIs to communicate and share security actions that may constitute key elements within an effective and layered approach to transportation security. Although voluntary, many of the applicable stakeholders are currently employing some of these security actions as evidenced by the results of Corporate Security Reviews (CSRs) HMC conducts. TSA

conducts CSRs on a voluntary basis with organizations engaged in transportation by motor vehicle and those that maintain or operate key physical assets within the highway transportation community. CSRs serve to evaluate and collect physical and operational preparedness information, critical assets and key point-of-contact lists, review emergency procedures and domain awareness training, and provide an opportunity to share industry best practices.

Another voluntary initiative is the Customs-Trade Partnership Against Terrorism (C-TPAT), which is a joint government-business cooperative relationship strengthening overall supply-chain and border security. Motor carriers must be validated by Customs and Border Protection (CBP) prior to receiving program benefits such as reduced customs inspections and reduced border delays.

The Automated Commercial Environment (ACE) is an electronic trade processing system operated by CBP to facilitate legitimate trade while strengthening border security. ACE provides the trade community, including importers, exporters, and transportation companies, with a single, centralized access point for communications and information related to cargo shipments.

4.4.6 International Initiatives

There are a few RMAs focused upon reducing risks in the international supply chain, and they meet at least one of the objectives of each of the four sector goals.

The Free and Secure Trade (FAST) program is a commercial clearance program for known low-risk shipments entering the United States from Canada and Mexico. This trusted shipper program is open to U.S., Canadian, and Mexican truck drivers and allows for expedited processing for commercial drivers who have completed background checks and fulfill certain eligibility requirements. Participation in FAST requires that every link in the supply chain, from manufacturer to carrier to importer, is certified under the C-TPAT program.

The Canadian Border Services Agency (CBSA) manages two programs that reduce risks in the international supply chain. The Partners in Protection (PIP) is the Canadian counterpart to C-TPAT. PIP membership is a prerequisite to participate in the FAST program. Although companies must apply separately for PIP and C-TPAT, both countries apply similar security standards and similar site validations when approving companies for membership in their respective trade security program. The Advance Commercial Information (ACI) is Canada's counterpart to ACE. ACI provides CBSA officers with electronic pre-arrival cargo information so that they are equipped with the right information at the right time to identify health, safety, and security threats before the goods arrive in Canada.

4.5 Performance Metrics

Measurement progress indicators vary across the HMC mode. Most security initiatives within this mode are predominately voluntary at this time. As such, most metrics are output-based while corresponding baselines are completed.

Plans to measure effectiveness are based upon collecting data and measuring it against the corresponding baselines established for initiatives within the RMA categories. Baselines are specific to each type of initiative. However, the commonality across initiatives is that once a baseline is established, any subsequent deviation from this baseline can be tracked to quantify a percentage of change, or an improvement that the RMA has achieved. Information collected must be verified, shared, and stored as appropriate in each case.

While it is feasible to measure and report on progress against stated goals, the sector may never be able to truly rate the effectiveness of some programs. The absence of a terrorist incident or a specific natural disaster does not necessarily mean that the RMAs have kept the incident from occurring or improved the sector's disaster response capabilities. Nonetheless, the HMC mode will continue to work collaboratively with its partners to complete the establishment of baselines and accurately report progress against its stated goals and objectives.



5. Security Gaps

Section 4 outlined the goals and objectives of the HMC mode to enhance security from all hazards. Some specific RMAs employed were described; however, there remain certain security gaps in the layered security approach among the sub-modes and the partners. Budgetary considerations and time needed for implementation are considerable constraints confronting Federal, State, local, and tribal government partners, as well as industry partners.

Within the highway transportation system, neither private industry nor security threats that confront it are static. The following gaps are equally manifested in varied and diverse complex and interconnected networks.

5.1 Security Plans

There is limited coordination among the States or the Federal Government for regional security and event planning. Additionally, unlike HAZMAT carriers, who are currently required to have a security plan, motorcoach carriers, school bus carriers, and State bridge and tunnel owners/operators currently are not subject to these regulatory requirements. Furthermore, no Federal grant funding is currently available to address school bus security, protection, or resiliency planning. Also, comprehensive planning for security at transshipment nodes is inadequate because these nodes are not sufficiently integrated into the sector's critical infrastructure.

5.2 Security Assessments and Methodologies

There are no standardized assessment methodologies that allow for a normalized result across the industry when used against standard planning templates and processes. There are dissimilar regulations between the carrier sub-modes regarding who will be required to have completed vulnerability assessments. No transportation employees, other than Commercial Driver's License (CDL) HAZMAT endorsement licensees, are required to be vetted, including CDL licensees with passenger endorsements, and those loading hazardous materials, dispatching vehicles, or maintaining vehicles. Coordination among differing Federal personnel security vetting initiatives is necessary to prevent a duplication of industry efforts and costs. There is no system or requirement to vet drivers/signees of commercial rental truck agreements. In addition, security assessments are needed for high-value, critical highway infrastructure, as well as grant funding specifically for highway infrastructure security initiatives.

5.3 Security Training

There is a lack of standard security training that is available or that can be customized by sub-mode. There are dissimilar regulations for the carrier sub-modes regarding requirements for employee security training.

5.4 Security Exercises

There is no effective way for carriers, who are currently required to have security plans, to test those plans with periodic security exercises.

5.5 Information Sharing and Communications

The current TSA alerts system does not contain all highway transportation carriers contact information. Due to hundreds of thousands of independent operators with no central office, and inconsistent communications capabilities from dispatch offices to drivers, HSIN is not an effective means to share information with a great deal of the industry. There is currently no system that exists to get time-sensitive security information to transportation drivers while on the road. There is also no current capability to ascertaining the number, location, and risk of vehicles carrying security-sensitive hazardous materials or critical goods, school buses with students on board, or motorcoaches during evacuation operations or in areas with ongoing security events.

An ongoing challenge is to consistently disseminate useful information to modal partners that is not constrained by confusing protection levels that restrict information sharing.

Another concern is the current First Observer® program is grant funded and has no annualized funding beyond FY2011.

6. Way Forward

The Federal agencies with responsibilities related to Highway Infrastructure and Motor Carrier protection are committed to implementing the NIPP and the Transportation Systems SSP thereby reducing or eliminating the security gaps identified in section 5. As the SSA for transportation security, TSA will work with private industry and government partners to develop a comprehensive strategy that looks holistically at the sector. Substantial challenges confront the SSA and all of the HMC partners, especially the size, diversity, and relatively unregulated operational security nature of the mode, when compared with the highly regulated aviation mode, for example. Private industry partners have a vested interest in implementing procedures that ensure the security of their enterprises and their customers and in adhering to the various rules and regulations that govern the mode.

Government agencies with roles and responsibilities in the Transportation Systems Sector must balance operational needs and requirements with resources. The SSA focuses on four key functional areas for improving the security and resiliency of the sector: security planning, conducting vulnerability assessments, training, and exercises. The HMC mode faces an ongoing challenge regarding information sharing, which calls for a willingness to fully support new initiatives and allowing them to mature. An all-hazards approach must be reflected in future funding of risk mitigation activities and security grants. Key areas intended to be addressed within the goals and objectives detailed in section 4.1 by the HMC mode within the next three years are described below.

6.1 Security Planning

Mindful of the National Response Framework guidance, Federal modal partners will improve their all-hazards approach on security planning initiatives. They will also develop new risk mitigation solutions to address risks from security gaps and cybersecurity threats. The sector's stakeholders propose that grant funding to address school bus security issues should be made available. Regulatory programs are planned to ensure that specific security planning challenges are addressed. This is particularly necessary for both the motorcoach industry and the Highway Security Sensitive Materials (HSSM) Carriers.

6.2 Security Assessments

The need for security assessments will remain for the foreseeable future. TSA is required by the 9/11 Act to update industry risk assessments and needs to further refine and standardize its own criteria for risk assessments. Assessments of critical highway infrastructure should be coordinated jointly between the Federal agencies responsible for security and the State and local governments who own these assets. Regulatory programs are required for motorcoach industry security vulnerability assessments per the 9/11 Act, and for specific HSSM carriers. Improved coordination between Federal agency partners should eliminate

dissimilar regulations. Likewise, there must be coordination of Federal personnel security vetting efforts to prevent duplication of industry efforts and costs.

6.3 Security Training

Per the 9/11 Act, security training is required for the motorcoach industry and a regulatory program is being developed to support this endeavor. TSA also plans to develop a regulatory program for HSSM carriers security training. These regulatory programs should be coordinated with other Federal agencies to avert promulgating dissimilar regulations. Finally, domain awareness security training should be expanded to service all of the HMC modes.

6.4 Security Exercises

Sector security training exercises are used by private industry and government partners to increase awareness, improve processes, and enhance partnerships. TSA will continue its deployment of I-STEP, specifically by developing an online, interactive capability to meet the particular needs of highway owners/operators. The interactive online training system is intended to allow private industry partners to participate in training exercises remotely and to provide a trial environment to assess their own individual security plans.

6.5 Information Sharing and Communications

Section 5 describes a key gap in security around the ability of government and authorized partners to effectively share actionable information. Addressing this gap requires procedural and systems activities. Requirements to address the gaps must be better understood and the sufficiency of current mechanisms such as TSA alerts, notifications, bulletins, and ISAC releases evaluated.

General communications between government and private stakeholders must continue to be promoted. Existing mechanisms such as conference calls, exercises, domain awareness activities, and the GCC/SCC process will continue and must incorporate an all-hazards approach. Sharing information across agency mission lines and modal sectors is critical in reducing the risk of transportation security threats and ensuring a coordinated and effective response to any domestic incidents.

The SCC and GCC have formed a Joint Information Sharing Environment Working Group to develop requirements, protocols and procedures to formalize information sharing within the sector. This institutionalized system is intended to share routine- and incident-related information as well as alerts, warnings, and notifications. Within the Information Sharing Environment, HMC partners will address the best mechanisms to share and use information in the most effective and efficient manner possible.

Appendix 1: Strategy for a National Highway Bridge Security Program

Introduction

There are approximately 600,000 highway bridges on public roads in the United States encompassing various sizes, designs, ownership, levels of historical significance, and vulnerability. Bridges represent an attractive target to terrorists because they offer a concentrated point of attack for terrorists wishing to disrupt commerce and freedom of movement within America and across its land borders and for the potential spectacular nature of a successful attack.

In the post-September 11 environment, the need for a strategy for securing highway bridges is apparent to responsible officials at all levels of government and throughout the highway bridge stakeholder community. An Al-Qaeda manual captured in 2001 identifies “blasting and destroying bridges leading into and out of cities” as one of the military missions of the terrorist organization. In 2003, the FBI learned of an aborted plot by an American Al-Qaeda operative, Iyman Faris, to cut the wire cables of the Brooklyn Bridge using a torch. The post-9/11 Blue Ribbon Panel of bridge and tunnel experts estimated that the cost of replacing a bridge or tunnel due to a large-scale terrorist attack could exceed \$10 billion.

Though not a terrorist act, the collapse of the I-35W Mississippi River Bridge in Minnesota on August 1, 2007, again called attention to the consequences associated with the destruction of a bridge. Accordingly, interagency representatives convened the Highway Bridge Security Strategy Working Group to coordinate the security efforts initiated by the respective segments of the Federal Government bridge community. The working group brings together the Departments responsible for bridge security and bridge safety—the Department of Homeland Security (DHS) and the Department of Transportation (DOT). The Transportation Security Administration (TSA) chairs the working group. Other members include the DOT Federal Highway Administration (FHWA), which along with the DHS Office of Science & Technology (S&T) and the DHS Office of Infrastructure Protection (OIP), provides technical expertise on bridge design, risk assessment methodology, and countermeasures. The purpose of this working group on bridge security is to identify the objectives that, when met, will provide a layer of security for the transit of people and goods across our country and borders.

Purpose

The purpose of this paper is to define a strategy for the Federal Government to address the security risks associated with highway bridges in the United States and recommend solutions. The proposed strategy will:

- Identify, assess, and prioritize risks to critical bridges from terrorist or criminal acts;
- Provide to bridge owners and operators standard means of risk assessment and risk mitigation based on threats, vulnerabilities, and consequences;

- Establish a means to prioritize available Federal security funding to address security gaps at the Nation's most critical bridge infrastructure;⁹
- Establish priorities for research and development and security enhancement projects over the long-term; and,
- Encourage and guide the incorporation of risk-reducing technologies and construction practices in improvements to existing bridges and future highway bridge design.

Background

Bridge resiliency is a responsibility shared by Federal, State, and local government agencies and the private owners and operators of many of the Nation's most important highway bridges. Federal partners include DOT, FHWA, DHS, TSA, S&T, OIP, the U.S. Department of Defense (DoD), and the U.S. Army Corps of Engineers. Security begins with the States, which establish requirements for highway bridge design, construction, maintenance, and replacement. Private bridge owner/operators, private industry, and organizations like the American Association of State Highway and Transportation Officials (AASHTO), which represents State Departments of Transportation, also share in the responsibility for designing, building, maintaining, and operating bridges that support the surface transportation network.

This strategy document represents the coordinated effort of the highway bridge security work group to capture situational awareness of the current state of highway bridge security and to guide the development and application of measures that will enhance bridge resiliency against a multitude of threats for years to come. Some of the initial effort has already been completed. Rather than duplicating previous effort, this strategy will draw heavily upon institutional knowledge and capabilities, and synthesize existing work toward clearly identified strategic ends.

Strategy

The strategy will be divided into three phases that collectively will yield enhanced security to critical bridges in the short-term, while guiding research, development and implementation in the medium- and long-term. Elements of the strategy will cut across phases, but the sequential order should clarify the relative priority of objectives.

Phase I will identify critical bridges, assess current risk, and implement short-term measures to mitigate that risk. During this phase, a list of the Nation's critical bridges will be developed and categorized into two priority tiers using existing TSA and other Federal data.¹⁰ This initial tiering will incorporate threat information and will be based on criteria such as traffic volume, collocation with other infrastructure, amount of time needed to rebuild, iconic value, existing vulnerability data, and the impact of loss on the local, regional, and national economy.

Next, existing strategic assessments—performed either privately or with Federal guidance—will be compiled and compared against the list, to determine which security gaps at tier 1 and tier 2 bridges have been previously identified and/or addressed.¹¹ The process will draw upon the TSA corporate security review (CSR) program, which serves to evaluate physical and operational preparedness information, collect critical assets and key point-of-contact lists, and review emergency procedures and domain awareness training. Information from site-assistance visits (SAVs) performed by the DHS OIP and by the FHWA Engineering Assessment Team will also be used.

⁹ At the time of this document's writing, dedicated sources of funding assistance for highway infrastructure security improvements/enhancements do not exist. References in this document to federal funding assume that such assistance will be made available.

¹⁰ The tier system referred to here applies only to bridges, and is based on criteria to be established by the work group. It does not refer to previous infrastructure tiers established by the Office of Infrastructure Protection, and is not meant to affect or replace that process.

¹¹ The work group recognizes that technologies currently in place to mitigate other hazards to bridges have security benefits.

The compiled information will establish the baseline for completing phase I of the bridge security strategy, which is to guide limited available resources to mitigate risk at the Nation's most critical bridges. The result will be an immediate and cost-effective boost to security against threats at the most vulnerable and potentially at-risk bridges.

During Phase II of the security strategy, DHS and DOT will provide recommendations to tier 1 and tier 2 bridge owners on the types of modifications that Federal funding will support as part of its effort to mitigate overall risk to the Nation's bridge infrastructure. This phase will also support and encourage scientific research to improve design technologies and assessment methodologies for the long-term.

To support this phase, the work group will establish standard risk assessment methodologies that can be implemented by bridge owners and operators to qualify for Federal funding. An appropriate methodology must account for the specific risks faced by each individual bridge, based on the critical elements of its design type (truss, suspension, cable-stay, etc.) and the adequacy of all hazards measures already in place. The CSR process identified above, the component-level risk management system supported by DOT, and the Multi-modal Risk Assessment Process supported by AASHTO are examples of market-ready processes that will be considered by the work group.

Standard methods of risk assessment may assist bridge owners and operators to access available Federal funding for projects aimed at mitigating risk. To the Federal Government, standardization provides a way to evaluate protective strategies and security enhancements that support the objective of national bridge security. Federal funds for bridges, contingent upon a risk assessment that considers threat, vulnerability, and consequences of a successful attack, serve as investments in long-term security.

The identification of standards for threat assessment in phase II must concurrently drive the scientific effort required to advance countermeasure development in the long-term. Such development should follow on the work started by the FHWA, DHS S&T, DoD, National Cooperative Highway Research Program of the National Academies, and in the private sector. As funding is directed to mitigate medium-term risk, research and development of new technologies and risk assessment methodologies will make the strategy viable in the long-term.

Phase III is the implementation of layered security measures at the Nation's most critical bridges, accompanied by the development and implementation of new design and retrofit measures for risk mitigation. During this phase, the working group of Federal agency subject matter experts will establish programmatic authority in an appropriate office. This office will be charged with overseeing and collaborating, as appropriate, to update the standards, methodologies, protective strategies, and technologies required by long-term implementation of the strategy.

Because a successful bridge security strategy is one that can dynamically adapt to changing threat scenarios and developments in technology, phase III should not be considered a final end-state. Its implementation, however, will establish a benchmark by which the security of existing and future highway bridges may be judged, against the prevalent threats of their times.

Objectives

This Strategy is guided by the following overall objectives:

1. Identify and prioritize the Nation's most critical highway bridges.
2. Identify gaps in security via standardized risk assessment tools.
3. Make available additional Federal funding to the most critical bridges, tying access to Federal dollars to implementation of standardized risk assessment processes.
4. Make additional funding available for research and development of design technologies and risk assessment methodologies that are viable for retrofit strategies, future design standards, and construction projects.

5. Establish programmatic authority to determine agreed-upon assessment methodologies, along with standard protective strategies and technologies.
6. Encourage and guide the incorporation of vulnerability-reducing technologies and construction practices in future highway bridge design, improvements, and enhancements.

Annex E: Freight Rail



Table of Contents

1. Executive Summary	281
2. Overview of Mode	283
2.1. Overview	283
3. Implementation Plan	291
3.1. Goals and Objectives	291
3.2. Strategic Risk	291
3.3. Tactical/Operational Risk	292
3.4. Decisionmaking Factors	294
3.5. Risk Mitigation Activities	294
3.6. Metrics for Continuous Improvement	297
4. Security Gaps	301
5. National Strategy for Freight Rail Transportation Security	303

List of Figures

Figure E3-1: The U.S. Railroad Network	293
Figure E3-2: Freight Rail TIH Risk Reduction	299
Figure E5-1: National Strategy for Freight Rail Transportation Security	304

List of Tables

Figure E5-2: National Strategy Crosswalk	308
--	-----



1. Executive Summary

Protecting the freight rail transportation system of the United States is essential to the Nation's security, public health and safety, economic vitality, and way of life. A successful terrorist attack on the U.S. freight railroad industry could significantly disrupt the functioning of government and private businesses alike, and cause cascading effects far beyond the targeted physical location. Such an attack could result in catastrophic losses in terms of human casualties, property destruction, and economic effects, as well as profound damage to public morale and confidence. The potential exists for the freight rail system to be the direct target of terrorism, or rail shipments of rail security-sensitive materials¹ (RSSM), including hazardous materials classified as toxic or poison inhalation hazards (TIH or PIH), could be used as a weapon of mass effect with devastating physical and psychological consequences.

The Secretary of Homeland Security, in accordance with Section 1511(a) of the 9/11 Commission Act,² delegated to the Transportation Security Administration (TSA) the responsibility to complete a nationwide risk assessment examining the potential threat, vulnerability, and consequence (TVC) of a terrorist attack on the Nation's freight rail system. TSA prepared the risk assessment in conjunction with other Department of Homeland Security (DHS) elements and Federal partners, as well as private sector stakeholders in the transportation sector, to identify potential gaps, determine risk-based priorities, and leverage security improvements. The risk assessment identified two primary risk areas in freight rail transportation:

- **The Movement of Cargo**
 - The potential for rail cargoes to be used as weapons of mass effect.
- **The Loss of Critical Transportation System Infrastructure**
 - The disruption or degradation of the freight rail network.

The diversity and expanse of the North American railroad system is extraordinary and presents a unique preparedness challenge to prevent, respond to, and recover from potentially devastating effects. Numerous passenger and commuter rail systems throughout the country operate at least partially over tracks or rights-of-way owned by freight railroads. The National Railroad Passenger Corporation (Amtrak), for example, operates on more than 22,000 miles of track owned by freight railroads through operating agreements.³ The interdependency of freight and passenger rail infrastructure – including common bridges, tunnels,

¹ Rail security-sensitive materials are defined as (1) A rail car containing more than 2,268 kg (5,000 lbs) of a Division 1.1, 1.2, or 1.3 (explosive) material, as defined in 49 CFR 173.50; (2) A tank car containing a material poisonous by inhalation as defined in 49 CFR 171.8, including anhydrous ammonia, Division 2.3 gases poisonous by inhalation as set forth in 49 CFR 173.115(c), and Division 6.1 liquids meeting the defining criteria in 49 CFR 173.132(a)(1)(iii) and assigned to hazard zone A or hazard zone B in accordance with 49 CFR 173.133(a), excluding residue quantities of these materials; and (3) A rail car containing a highway route-controlled quantity of a Class 7 (radioactive) material, as defined in 49 CFR 173.403. See 49 CFR 1580.3 and 1580.100(b).

² "Implementing Recommendations of the 9/11 Commission Act of 2007" (Public Law 110-53, August 3, 2007), Section 1511(a).

³ In addition, many commuter rail systems operate primarily or exclusively over tracks or rights-of-way owned by freight railroads.

and tracks – also increases the likelihood that incidents affecting highly critical assets could affect the entire railroad system. The rail network is vast and the owners/operators vary in size and communities served. Preparedness, therefore, is a shared responsibility between government entities and the private sector. Government agencies, the private sector railroad carriers, and other stakeholders must be positioned to meet the Nation's needs to strengthen preparedness, security, and resiliency in the freight rail sector.

2. Overview of Mode

2.1 Overview

There are approximately 140,000 miles of active railroad track in the United States. A total of 565 common carrier freight railroads use these tracks, and they earned \$63 billion in revenue in 2008.⁴ Of the common carrier freight railroads, there are seven Class I freight railroads⁵ that generate a minimum operating revenue of \$401 million. Though they comprise only 1 percent of all railroads, Class I carriers operate on over 94,000 miles of the total track in the United States (67 percent). Of the approximately 180,000 employees among all carriers, Class I railroads employ over 164,000 persons and generate over \$59 billion or 93 percent of the total revenue.⁶ These railroads operate over large areas, in multiple States, and concentrate on the long-haul, high-density, intercity traffic lines.

The remaining 558 carriers are commonly referred to as regional and short line railroads, but are also known as Class II and III carriers. Regional railroads are classified as operating on at least 350 miles of active lines and having revenues between \$40 and \$400 million. Short line railroads are carriers operating on less than 350 miles of line and generating less than \$39 million in annual revenues. Short line railroads can be further divided into local line-haul railroads and switching/terminal railroads. Switching and terminal carriers operate primarily in a localized territory and provide connecting services between carriers in major cities. Terminal railroads are often owned by one or more of the Class I carriers. In several major metropolitan areas, a loss of service from a belt railroad (a type of short line) or terminal railroad would cause a disruption in interchange operations between eastern and western Class I rail carriers.

Freight railroads serve nearly every industrial, wholesale, retail, and resource-based sector of the U.S. economy. With a network that runs from one end of the country to the other, freight railroads work to connect businesses with each other across the United States and with markets overseas. In 2007, freight railroads generated \$91.459 billion in the U.S. goods trade with Canada and Mexico.⁷ About 30,362 trains crossed into the United States from Canada, while 10,648 trains crossed in from Mexico.⁸ Freight railroads are responsible for transporting a majority of goods and commodities that Americans depend on, hauling everything from lumber to vegetables, coal to orange juice, grain to automobiles, and chemicals to scrap iron. One

⁴ Association of American Railroads. *Railroad Facts*. 2009 Edition.

⁵ For purposes of accounting and reporting, the Surface Transportation Board (STB) groups freight railroad carriers into three classes. The STB is an economic regulatory agency that Congress charged with the fundamental missions of resolving railroad rate and service disputes and reviewing proposed railroad mergers. See ICC Termination Act of 1995, Pub. L. 104-88, 109 Stat. 803 (December 31, 2005).

⁶ Association of American Railroads. *Railroad Facts*. 2009 Edition.

⁷ U.S. Department of Transportation, Research and Innovative Technology Administration, Bureau of Transportation Statistics, *TransBorders Freight Data*, available at <https://www.bts.gov/ntda/tbscd/prod.html> as of August 2008.

⁸ U.S. Department of Transportation, Research and Innovative Technology Administration, Bureau of Transportation Statistics, *Border Crossing/Entry Data*, available at <http://www.bts.gov/itt/> as of September 2008.

example of the critical role that freight railroads play in the support of other sectors is that of the Energy Sector. Coal is the fuel that generates half of America's electricity. Freight railroads are responsible for the transportation of more than 70 percent of all U.S. coal shipments (7.7 million carloads in 2008).⁹ The Energy Sector relies on the railroad network to deliver the vast quantities of coal required for power generation. While products like coal do not pose a threat if spilled or released, the disruption of the rail system could adversely impact other critical sectors depending on the location of the disruption. And although coal, like the majority of freight railroad shipments, poses little or no threat to civilian populations and consequently has little or no target value to terrorists, there are other commodities that, when released from their shipping containers, have the potential to cause widespread casualties.

Approximately 101,000 shipments¹⁰ of TIH materials are transported by rail each year. Ninety percent of that volume comes from six chemicals – anhydrous ammonia, chlorine, ethylene oxide, anhydrous hydrogen fluoride, sulfur dioxide, and anhydrous hydrogen chloride. Chlorine and anhydrous ammonia are the most frequently transported and constitute 78 percent of all TIH rail shipments. A successful deliberate terrorist attack against TIH materials in transportation poses serious risks of fatalities and injuries. Two accidents demonstrate the devastating and lethal consequences following a release of TIH from a rail car in transit. In Graniteville, South Carolina in January 2005, a train collision and derailment on a siding resulted in a release of 56.3 tons of chlorine. Nine people died as a result of the chlorine gas, while over 5,400 people were evacuated within a one-mile radius and at least 200 were treated for respiratory complaints. Near Macdonia, Texas, in June 2004, a train collision and derailment resulted in a chlorine release of 54 tons. Three people were killed by the chlorine gas and at least 30 civilians were treated for chlorine exposure.¹¹ Though these incidents were caused by accidental releases, they demonstrate the type of impact that a large scale release of a TIH material can cause. These harmful effects would potentially be magnified in a highly populated urban area.

According to the U.S. Department of Transportation (DOT) Bureau of Transportation Statistics, hazardous materials (HAZMAT) traverse more than 72 billion ton-miles on rail.¹² But despite the risks, hazardous materials are essential to the functioning of the economy and society. These materials fuel motor vehicles, purify drinking water, and heat and cool homes and offices. Other hazardous materials are used for farming and medical applications, manufacturing, mining, and other industrial processes.

Federal law requires freight railroads to carry all shipments (including TIH) that are tendered in accordance with DOT regulations. Radioactive materials, which are classified as hazardous materials, are also transported by rail. The Nuclear Regulatory Commission and the Department of Energy have primary security oversight for these shipments.

Railroads are also one link in the U.S. intermodal supply chain. Over the past 10 years, intermodal traffic has been the fastest growing rail traffic segment. Today, there are 9.2 million intermodal rail shipments annually. An increasing number of the intermodal shipment transfers from the maritime mode to freight rail are international movements.

Assets, Systems, and Networks Including Cyber Networks

The current freight rail system is a diverse network of companies, both large and small; these carriers compete and cooperate economically with one another. Since there is not one single coast-to-coast freight rail operator, these carriers have developed

⁹ "The Economic Impact of America's Freight Railroads." Association of American Railroads. May 2009. Web 07 August 2009, available at <http://www.aar.org/InCongress/~media/AAR/BackgroundPapers/EconomicImpactofUSFreightRRs20May2009.ashx>.

¹⁰ Shipments is a loaded origination.

¹¹ National Transportation Safety Board. (RAR-06/03, PB2006-916303, July 6, 2006). *Railroad Accident Report: Collision of Union Pacific Railroad Train MHOTU-23 with BNSF Railway Company Train MEAP-TUL-126-D with Subsequent Derailment and Hazardous Materials Release, Macdonia, Texas, June 28, 2004*. Washington, D.C.

¹² 2002 Commodity Flow Survey – Hazardous Materials. "Table 1a. Hazardous Material Shipment Characteristics by Mode of Transportation for the United States: 2002." Bureau of Transportation Statistics, December 2004. p.19.

various interchange, joint services, and voluntary access agreements that allow for the transfer of rail cars between carriers, as well as the operation of one carrier's train on the tracks of another railroad. The result is the rapid and efficient movement of commodities and finished goods throughout the Nation.

In the event of major natural disasters, railroads have demonstrated resilience in bringing assets and infrastructure back online in a timely manner. As demonstrated during Hurricanes Katrina and Rita and then with Ike and Gustav, in Louisiana and Texas, the rail industry, although severely impacted on a local basis, was able to continue the flow of traffic through other areas of the country using well-planned detours. The railroad operations centers oversee current conditions to determine if a hazard, such as adverse weather conditions, is pending, and then take the corrective actions to avoid disruptions and/or restore operations as quickly as possible.

The same operations model would be applied to a catastrophic incident involving a terrorist attack on a TIH tank car or if a critical infrastructure asset is lost (e.g., a bridge). The national network of carriers is designed for greater resiliency in the system. If required, carrier operations centers can divert trains if portions of the freight rail system are rendered inoperative (e.g., train derailments or washouts), allowing for the continued transportation of freight with minor delay. With this in mind, it is imperative that efforts to improve security for the system are adapted to this environment and are equally applied to all freight rail carriers.

Railroads also provide critical support to the Department of Defense (DoD). DoD designated more than 30,000 miles of rail line as the Strategic Rail Corridor Network that provides the backbone for transporting DoD shipments. This network is essential to the movement of specialized equipment and large quantities of material required to support military operations and national defense.

With the merger of information system technology and transportation infrastructure, railroad operations have become increasingly reliant on information systems and communication technologies. Rail companies have made growing use of onboard computers, local area networks, automated equipment identifiers, global positioning system (GPS) tracking, automatic reporting of work orders to headquarters, car scheduling and train order systems, and two-way wireless connections.¹³ Commercial fiber-optic communications cables are also laid along rights-of-way. These are commercial lines, used by various commercial users as well as railroads. The rails themselves are also used as communications channels for signal controllers and trackside signals. Nearly all locomotives and rail cars are tagged with automatic identification transponders, which automatically record and report car location as it passes a wayside detector. As a result, the standing orders of cars are verified automatically, and car location reports are transmitted to railroad service centers and customers faster and more accurately.¹⁴

The railroad's growing dependence on these centralized monitoring and control systems, including Centralized Traffic Control networks, prompts concerns of possible cyber attacks upon these systems. Although there is no evidence of a specific terrorist threat to freight rail cyber systems, intelligence reporting indicates al-Qaeda and other adversaries with ill intent have a sustained interest in launching operations against computer networks. The Federal Government, in cooperation with the industry, continues to identify efforts to address gaps in rail security, which include cybersecurity challenges, through conferences and security briefings.

¹³ Association of American Railroads. 2003. *Facts About Railroads*. Policy and Economics Department, Jan. 10. www.aar.org/PubComments/Documents/AboutTheIndustry/Statistics.pdf.

¹⁴ National Research Council (U.S.) Committee on Freight Transportation Information Systems Security. "Transportation Research Board Special Report 274. – Cybersecurity of Freight Information Systems: A Scoping Study." 2003. Washington, DC. p. 23.

Risk Profile

The fundamental challenge to securing the freight rail network is to protect against a constantly changing, unpredictable threat environment without impeding the continuous movement and free flow of commerce that is required in today's just-in-time supply chain. Attacks can be isolated, having minimal effect on the total railroad operating system, or can result in a major impact that has national implications, potentially shutting down railroad operations for specific sectors and lasting several weeks to months. The Transportation Security Administration's Office of Intelligence (TSA-OI) "Annual Threat Assessment to Freight Rail" report, dated September 15, 2009, indicates that while there is no specific threat or intelligence pointing to freight rail transportation, the possibility exists that the freight rail system could be a target for terrorists.

In assessing the security risk to the freight rail network, it is important to remember that the freight rail system was designed with ease of access as a fundamental principle that underlies its operational success. TSA risk assessment efforts entail examining the critical assets, such as bridges, tunnels, and yards, that are required for carrying out the freight railroad's basic mission of moving freight. Rail yards and terminals represent the fixed points in the network of railroad assets at which cars are transferred from one train to another, inspected and repaired as necessary. The movements of RSSM through freight rail facilities, or over open tracks, leave railroad employees and public populations vulnerable if confronted with the threat of a terrorist attack.

Intelligence reviews of various attacks worldwide, as well as analysis of seized documents, and the interrogation of captured and arrested suspects, reveal that there has been historic interest in carrying out attacks on railroad systems. The greatest interest shown by terrorist organizations, as evidenced by actual attacks, seized documents, and interrogations, has been attacks on passenger rail systems. This is because of the potential for larger civilian casualties, the relative ease of carrying out such attacks, and the potential to initiate panic in the general population. TSA-OI concludes that long stretches of open, unattended track and numerous critical points (e.g., junctions, bridges, contiguous passenger rail sites) that are difficult to secure make the U.S. freight rail system an attractive target for terrorist attacks.

While the potential is considered a low to moderate risk, documented evidence does exist that disgruntled persons have tampered with tracks.¹⁵ Control systems are also vulnerable to attack either by terrorists or acts of vandalism. However, the fail-safe nature of freight rail control systems may serve to mitigate the risk of a catastrophic incident.

Risk Assessment Defined

At TSA, a risk assessment is a product or process which collects information and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decisionmaking. It is an appraisal of the risks facing an entity, asset, network, geographic area, or other grouping. For example, TSA analysts have produced a risk assessment outlining risks to the freight rail industry. The product is called the Rail Security Risk Assessment (RSRA).

Methodology

To assess the risks of terrorism associated with freight rail, TSA uses a mix of qualitative and quantitative approaches consistent with risk assessments from other transportation modes.

For the RSRA, TSA established a team of risk management and security experts within the freight rail transportation system. TSA used the specialized experiences and backgrounds of these risk experts, coupled with the results and findings from risk methodologies and assessments throughout the Department of Homeland Security (DHS) (such as the National Comparative Risk Assessment, Strategic Homeland Infrastructure Risk Assessment, and the ongoing Transportation Sector Security Risk Assessment), as well as published reports from the Government Accountability Office regarding risk management approaches.

¹⁵ DHS, Transportation Security Administration (TSA) Office of Intelligence (OI). (U) *Freight Rail Threat Assessment*. Washington, D.C., May 13, 2008. pp. 2, 5-6.

TSA determined that a scenario-based approach was the most appropriate methodological tool to use for the RSRA. TSA applied the generally accepted risk management framework of risk as a function of TVC.

Purpose

After risks are assessed, requirements designed to address the risks can be developed. A suite of potential solutions that includes, but is not limited to, industry action items, grants, regulations, and security countermeasures can be formulated from the requirements.

The purpose of the RSRA is to describe the strategic-level risks to the railroad mode and to support TSA's Transportation Sector Security Risk Assessment (TSSRA), an overarching, strategic, scenario-based, cross-modal risk assessment based on TVC. TSA developed this assessment tool to further inform DHS leadership of security priorities, support strategic risk analysis processes, and help security experts prioritize transportation assets. The output of the RSRA is an important component of the TSSRA.

Sector Partners and Information-Sharing Mechanisms

The TSA Freight Rail Security Division (Division) regularly communicates with its stakeholders, implementing a variety of mechanisms to enhance its stakeholder relationships to effectively respond to issues, questions, or concerns regarding freight rail security. The Division has reached out to industry stakeholders, as well as those in Federal, State, local, tribal, and territorial governments. The Division shares open source, For Official Use Only, Law Enforcement Sensitive, and classified information where appropriate, and develops the content for and hosts pertinent, regular conference calls for internal and external stakeholders as needed. Meetings with the Freight Rail Government Coordinating Council (GCC) are also held once every quarter. The Division also meets with State Homeland Security Advisors to discuss current programs, as well as to solicit feedback on ways to enhance freight rail security in their region.

As described in the Transportation Systems Sector-Specific Plan (SSP), the Sector Coordinating Council (SCC) is the vehicle for industry stakeholders to coordinate and collaborate with TSA. The Division interacts with both the Freight Rail SCC and the Chemical SCC. The Freight Rail SCC is primarily composed of representatives from the freight railroads, while the Chemical SCC includes representatives from rail shippers and receivers. Both groups have a vested interest in the formation of initiatives and policies to reduce security risk in freight rail transportation.

Freight Rail GCC Membership

Department of Homeland Security:

- Transportation Security Administration (Chair)
- National Protection and Programs Directorate
- Federal Emergency Management Agency, Office of Grants and Training
- Office of Intergovernmental Affairs
- U.S. Coast Guard
- Customs and Border Protection

Department of Transportation:

- Federal Railroad Administration
- Pipeline and Hazardous Materials Safety Administration
- Surface Transportation Board

Department of Justice:

- Federal Bureau of Investigation

Department of Defense:

- Assistant Deputy Under Secretary of Defense (Transportation Policy)

Freight Rail SCC Membership

- Association of American Railroads (Co-Chair)
- American Short Line and Regional Railroad Association (Co-Chair)
- Amtrak[®]
- Anacostia and Pacific
- BNSF Railway Company
- Canadian National
- Canadian Pacific Railway
- CSX Transportation
- Genesee & Wyoming
- Iowa Interstate Railroad, Ltd.
- Kansas City Southern Railway Company
- Metra[®]
- Norfolk Southern
- RailAmerica, Inc.
- Union Pacific Railroad Company
- Wheeling & Lake Erie Railway

Numerous programs and initiatives exist to engage private sector partners in collaborative efforts to reduce security risk. The Division consistently strives to transmit pertinent security information to its stakeholders in a timely manner. Consequently, the Rail Security Coordinator (RSC) Network has become the primary vehicle for information sharing. Whereas TSA initially had a partial picture of its stakeholders in the freight rail industry, the RSC Network presents a comprehensive population of rail carriers, shippers, and certain receivers of rail security-sensitive materials, allowing for effective outreach in regard to freight rail security issues. Further information about the RSC Network, as well as the freight rail portal on the Homeland Security Information Network (HSIN), is detailed below.

Rail Security Coordinator Network

On November 26, 2008, TSA issued a final rule on rail transportation security (see 73 FR 72130) which included provisions for freight rail carriers, RSSM shippers, and RSSM receivers operating within a High Threat Urban Area (HTUA)¹⁶ to appoint a primary and at least one alternate RSC.¹⁷ Designated at the corporate level, RSCs serve as the primary contact for intelligence

¹⁶ High Threat Urban Area (HTUA) means an area comprising one or more cities and surrounding areas including a 10-mile buffer zone. (see Appendix A to 49 CFR Part 1580).

¹⁷ 49 CFR 1580.101.

information and security-related activities and communications with TSA, 24 hours a day, 7 days a week. Covered entities are required to submit to TSA the contact information of each of their RSC designees, including names, titles, telephone numbers, and e-mail addresses. As such, TSA has assembled a comprehensive database of stakeholder contact information to establish a network for information sharing with the industry.

RSCs serve as the security liaison between their organization and TSA. They are a primary point of contact for receiving communications and inquiries from TSA concerning threat information or security procedures, and for coordinating responses with appropriate law enforcement and emergency response agencies. In the event that TSA needs to convey time-sensitive security information to a regulated party, the RSC Network is beneficial, particularly in situations requiring frequent information updates. The ability to communicate with specific individuals also allows for continuity. Individuals serving as RSCs are best suited to understand security problems, raise issues with corporate leadership, and recognize when emergency response action is appropriate.

The RSC Network is intended to benefit both the industry and TSA. By creating channels of communication between the private sector and the Federal Government, security and threat information can be shared more effectively. Establishing these communication channels provides TSA and industry with a broader view of the risks facing the sector, and allows for appropriate steps to be taken to prevent, deter, and minimize the consequences of a potential terrorist attack. The RSC Network was created with the intent to foster information sharing and thereby enhance the security of the sector.

Homeland Security Information Network

HSIN aims to share information in an integrated, secure, Web-based approach, as well as coordinate and collaborate with the Division's security partners in "real time." The Fiscal Year (FY) 2010 launch of the Freight Rail portal will integrate lessons learned in an effort to create a user-friendly tool to enhance information sharing. The Freight Rail portal on HSIN endeavors to be a "one-stop" shop to all of the Division's security partners. The portal is intended to be used as a way to provide consistent messaging on issues and topics related to freight rail security. The portal also connects users to other information resources, including the Transportation Security Information Sharing and Analysis Center (TS-ISAC). TSA will continue to develop and identify content, and facilitate maintenance of the portal, in order to augment its information-sharing capability with its stakeholders.

Railroad Alert Network

Since 2001, the Association of American Railroads (AAR) Security Operations Center has provided 24/7 security support to include threat warning and incident reporting. The security operations center supports the Railroad Alert Network (RAN), and provides oversight and direction to the Surface Transportation ISAC (ST-ISAC).

Building on the direction in Presidential Decision Directive 63, Homeland Security Presidential Directive 7 encourages the creation of private sector ISACs to protect privately-owned critical infrastructure from attack. At the request of DOT, the ST-ISAC was formed in 2003 by the AAR. The RAN provides oversight and direction to the ST-ISAC.

The ST-ISAC provides a secure cyber and physical security capability for owners, operators, and users of critical surface transportation infrastructure. Security and threat information is collected from worldwide resources, then analyzed and distributed to members to help protect their vital systems from attack.

The ST-ISAC also provides a vehicle for the anonymous or attributable sharing of incident, threat, and vulnerability data among the members. Members have access to information and analytical reporting provided by other sources, such as U.S. and foreign governments, law enforcement agencies, technology providers, and international computer emergency response teams.



3. Implementation Plan

3.1 Goals and Objectives

The Transportation Systems Sector has outlined four goals for the six modes: aviation, freight rail, highway and motor carriers, maritime, mass transit and passenger rail, and pipelines. Each goal is supported by objectives that assist in focusing each mode's respective programs and initiatives to meet that specific goal.

Goal 1: Prevent and deter acts of terrorism using, or against, the transportation system.

Terrorists may use attacks to directly disrupt the freight rail transportation system or they may use the cargo transported by a railroad to carry out larger attacks against the American people. The sector aims to prevent and deter terrorist attacks before they happen without disrupting the free flow of commerce or compromising civil liberties.

Goal 2: Enhance the all-hazard preparedness and resilience of the global transportation system to safeguard U.S. national interests.

The resilience of the freight rail mode can be improved by increasing its ability to accommodate and absorb damage from natural disasters or terrorist attacks without catastrophic failure. Resilience-improving strategies include a wide variety of mitigation activities, including support of response and recovery activities.

Goal 3: Improve the effective use of resources for transportation security.

Minimizing unnecessary duplication of efforts, improving coordination, and aligning resources to address the highest risks of the sector will improve the effective use of resources.

Goal 4: Improve sector situational awareness, understanding, and collaboration.

Strengthen partnerships to further national interests.

3.2 Strategic Risk

TSA's freight rail strategy is risk-informed, meaning risk is determined through Rail Corridor Assessments (RCA), critical infrastructure assessments, Corporate Security Reviews (CSR), intelligence analysis, and objectively-measured risk metrics. Using these tools, TSA employs a combination of voluntary guidelines and mandatory requirements to improve railroad security. The overall strategic risk objective of the TSA program is to build a safer, more secure, and more resilient freight rail industry. This is achieved by enhancing protection of freight rail cargo shipments and critical infrastructure to prevent, deter, neutralize,

and mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them. TSA programs also aim to strengthen freight rail preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency.

On November 26, 2008, TSA issued a final rule (see 73 FR 72130) on rail transportation security covering (in pertinent part) freight railroad carriers, shippers of RSSM, and receivers of RSSM located within an HTUA. The rule establishes procedures for positive chain of custody while TIH cars are in transportation, the appointment of Rail Security Coordinators, the reporting of location and shipping information of RSSM rail cars, and the reporting of significant security concerns to TSA. The Pipeline and Hazardous Materials Safety Administration (PHMSA), on the same day, issued a final rule (see 73 FR 72182) designed to enhance the security of shipments of hazardous materials. The rule requires rail carriers to analyze safety and security risks along rail routes where certain quantities of TIH, explosive, and high-level radioactive materials are transported, assess alternative routing options, and select the practicable routes that pose the least overall risk to safety and security. The PHMSA rule also clarifies rail carriers' responsibility to address within their security plan issues related to en route storage and delays in transit. Rail carriers are also required to inspect placarded hazardous materials rail cars for signs of tampering or the presence of suspicious items, including improvised explosive devices (IEDs).

The freight railroads have also undertaken efforts to enhance the security and resiliency of the freight rail transportation system. After the attacks of September 11, 2001, the AAR developed the Terrorism Risk Analysis and Security Management Plan that serves as both an industry-focused national plan and a template for each carrier to develop its own security plan. The Plan, last updated in 2009, encompasses the principles of threat and risk assessment by addressing five major functional areas identified by the industry: (1) hazardous materials, (2) operational security, (3) physical infrastructure, (4) military liaison, and (5) information technology and communications. In addition to the implementation of baseline countermeasures, the Plan specifies specific security actions at four threat-based alert levels to be taken by railroad police, operations security officials, and information technology security officials. The Plan supports TSA's strategy to reduce the risk associated with cargo shipments, critical infrastructure nodes, links, and flows of the network.

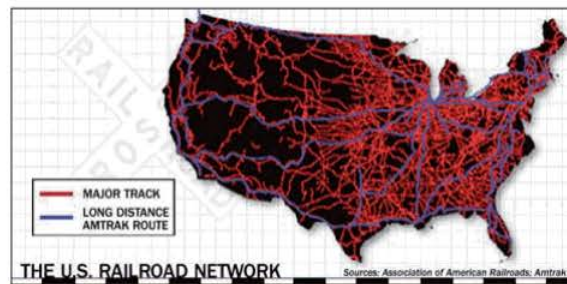
TSA and industry security partners use threat analysis to complete comprehensive risk assessments and risk mitigation activities. The risk management framework strikes a balance between developing ways to mitigate both specific and general threats. The framework permits the range of plausible attack scenarios to be broad enough, yet also contains sufficient detail to enable quantitative and qualitative risk assessments and definable actions and programs to enhance resiliency, reduce vulnerabilities, deter threats, and mitigate potential consequences.

3.3 Tactical/Operational Risk

The United States is an open, technologically sophisticated, highly interconnected, and complex nation with a wide array of infrastructure that spans important aspects of government, economy, and society. Efficient operation of the interstate freight rail network requires a uniform nationwide approach to railroad security. In assessing the freight rail system, TSA examines the network as a whole, as well as component parts of cargo and infrastructure. While each system component has its own security challenges, there are common vulnerabilities and mitigation strategies.

The great diversity and redundancy of the Nation's rail transportation system provides for significant physical and economic resilience in the face of terrorist attacks, natural disasters, and other disruptive incidents, and contributes to the unprecedented strength of the Nation's economy. However, this vast and diverse aggregation of interconnected assets, systems, and infrastructure also presents an attractive array of targets to terrorists. The majority of the freight rail network assets and systems are owned and operated by the private sector and some can be considered nationally critical infrastructure and key resources (CIKR).

Figure E3-1: The U.S. Railroad Network



TSA uses a comprehensive strategy that applies a common methodology across all transportation networks, regardless of mode, to address risk. Risk is assessed as a function of threat, vulnerability, and consequence.

$$\text{Risk} = f(\text{Threat, Vulnerability, Consequence})$$

The risk management framework is tailored and applied on a freight rail asset, system, network, or functional basis. The purpose of TVC assessments is to focus efforts on and highlight risk areas. Since September 2001, many Federal agencies and industry partners have been involved in significant efforts to identify the highest risk areas for TSA's security focus. Thus far, TSA and industry efforts have centered on analyzing threats, assessing vulnerabilities, and calculating the consequences of potential terrorist attacks. TSA's ongoing analysis is focused on the highest risk areas for freight rail that are deemed nationally critical. As such, TSA has determined that the two main risk areas in freight rail security which pose the greatest threat to life and property are:

- **The Movement of Cargo**

- The possibility that rail cargoes can be targeted in order to cause a large release of a TIH material or a material with explosive or radioactive properties with the intent to cause large scale civilian casualties.
- The potential for shipments of vital commodities to be adversely affected. Specifically, there is concern that rail cargoes may be tampered with or stolen for use in future terrorist or criminal acts including the following:
 - › The threat of a diversion of materials that could be used directly as weapons (e.g., DoD shipments of arms and ammunition);
 - › Materials that could be used in the manufacture of a weapon (e.g., ammonium nitrate); or
 - › Other commodities that could be tampered with, including the adulteration of food shipments affecting humans or for livestock.

- **A Direct Attack Upon Critical Rail System Infrastructure**

- With the intent to disrupt and degrade the freight rail system; and/or
- The intent to cause large civilian casualties.

3.4 Decisionmaking Factors

The management of TSA's strategic risk objective program focuses on identifying those elements in the freight rail industry with the highest relative risk and then the prioritization of protection initiatives and investments across the freight rail mode that will effectively reduce that risk. The past, ongoing, and future assessment efforts of TSA focus on risk management for the freight rail network. These have been, and will continue to be, a collaborative effort between the private sector; other Federal agencies; State, local, tribal, and territorial governments; and nongovernmental organizations. These efforts will lead to the prioritization of protection initiatives and investments across the freight rail sector, as well as the development of new CIKR protection efforts. They are also meant to cause resources to be applied where they offer the most benefit for mitigating risk by lowering vulnerabilities, deterring threats, and minimizing the consequences of terrorist attacks and other incidents.

3.5 Risk Mitigation Activities

TSA and its partners in transportation security have developed numerous processes, tools, and programs to measure and then reduce the risk to the freight rail sector. The following provides a summary of these programs.

Prevent and deter acts of terrorism using, or against, the transportation system

- **TIH Risk Reduction Program:** The freight rail vulnerability assessments have led to the implementation of a TIH Risk Reduction Program. The Program objectives focus on loaded and unattended toxic inhalation hazard material rail cars in HTUAs. The original risk reduction goal for this project was a 50 percent reduction in the risk associated with TIH rail shipments within HTUAs by the end of calendar year 2008. This goal was exceeded with a recorded reduction in risk of over 59%. In 2009 there was a cumulative risk reduction of over 82 percent as compared against the baseline year. The risk reduction was achieved because of the actions of the rail carriers and their customers' collaborative efforts—without legislation, regulations, or security directives.
- **Security Action Items:** TSA has, in conjunction with DOT and the Class I carriers, developed a program identifying a list of best practices called Security Action Items (SAIs). The 24 SAIs were issued as voluntary security guidelines for the transportation of TIH materials, and the set of guidelines was distributed to rail carriers and Federal partners in June 2006. These SAIs covered a broad range of security practices at both the corporate and field operational levels and addressed three general areas: system security, access control, and en route security.
- **Supplemental Security Action Items:** In November 2006, TSA issued three Supplemental SAIs which directly addressed issues of:
 - Expediting movement of TIH materials by reducing the number of hours TIH cars and trains are held by railroads in HTUAs;
 - Minimizing the occurrence of unattended TIH cars in HTUAs by implementing “positive control” of TIH through the development of site-specific plans and procedures for the positive and secure handoff of TIH cars at point of origin, destination, and interchange in HTUAs;
 - Identifying secure storage areas for TIH cars; and
 - Limiting the movement of TIH materials near public venues during National Special Security Events.

Enhance the all-hazard preparedness and resilience of the global transportation system to safeguard U.S. national interests

- **TSA Rail Corridor Assessments:** RCAs are fact- and risk-based and focus on assessing the vulnerabilities of high-population areas where TIH materials are moved by rail in significant quantities. They are conducted by teams comprised of subject matter experts from TSA, the affected railroads, and State and local homeland security officials. These assessments aid DHS in

identifying security control points (areas of high consequence and vulnerability) at each location. The security/critical control points are reviewed using current threat scenarios, and mitigation strategies are then proposed. After completing the assessment, the team prepares a summary of each corridor and a freight rail hazard analysis. The assessments provide site-specific mitigation strategies and lessons learned, as well as tactics that can be modified for use at the corporate or national level.

TSA fact- and risk-based RCAs identify operational practices and conditions that may result in heightened risk. The results of the HTUA assessments supported the development of the SAIs issued by DHS and DOT on June 23, 2006. RCAs have also served as the factual and analytical baseline for the SAIs and the Rail Security Notice of Proposed Rulemaking (NPRM). RCAs completed to date include: Washington, D.C., Northern New Jersey, Cleveland, New Orleans, Houston, Buffalo, Oklahoma City, Sacramento, Baltimore, Denver, Charlotte, and Las Vegas. Corridor Assessments are underway in Milwaukee, Memphis, Columbus, and Atlanta.

- **TSA Comprehensive Reviews:** Comprehensive Reviews (CR) are a larger-scale, more-encompassing version of the RCA. CRs provide a thorough evaluation of the security of a specific rail corridor and a comparative analysis of risk across transportation modes and critical infrastructure sectors in the specific geographic area. The team composition is increased to include response and recovery officials from all levels of government and DHS personnel, including assault planners, so that additional expertise, perspectives, and analyses are brought into the decisionmaking process, and security grant dollars are more effectively targeted. CRs have been performed in Northern New Jersey, Los Angeles, Chicago, and Philadelphia.
- **DHS S&T Rapid Response and Recovery Project:** In August 2008, the DHS Science and Technology Directorate (S&T) signed a Technology Transition Agreement, with the DHS Office of Infrastructure Protection and TSA, to develop technologies and methodologies that will reduce or eliminate the release of TIH materials from rail tank cars and stationary tanks, with potential approaches to include sealing and puncture resistant technologies. This work continues, in part, with the work initiated in the Tank Car Hardening Project (also known as “Dragon Shield”). TSA intends to work closely with DHS S&T on this project in determining ways TIH material rail tank car manufacturers can provide protection against some of the expected weapon threats to the rail tank car. Funding is anticipated from FY 2009 through FY 2014.

Improve the effective use of resources for transportation security

- **Intermodal Security Training & Exercise Program:** The Intermodal Security Training and Exercise Program (I-STEP) is being utilized by TSA’s Office of Transportation Sector Network Management (TSNM) for conducting transportation security exercises. TSA is applying the highly successful processes created under the Port Security Training Exercise Program (PortSTEP) to the multi-modal Transportation Systems Sector through I-STEP. TSA developed I-STEP in an effort to enhance the preparedness of the Nation’s surface transportation network. I-STEP is designed to address the unique transportation security issues found in the intermodal environment of the Nation’s transportation security network. The I-STEP exercises conducted by the Division facilitate discussions regarding the information-sharing processes and coordination between the Federal Government and the freight rail industry, particularly during heightened states of alert. The Division and I-STEP have analyzed the diverse characteristics of the freight rail system to provide the right combination of tools and exercise services to address these variations. To date, I-STEP freight rail security exercises have been conducted in Northern New Jersey, Chicago, Los Angeles, and St. Louis.
- **Bridge Criticality Tool:** The Division has developed a critical infrastructure risk assessment tool for freight rail bridges. This tool is designed to measure the criticality and vulnerability of freight rail bridges in the United States and will serve as the factual and analytical baseline to develop and propose security enhancements and mitigation strategies for critical railroad infrastructure. TSA planned to perform assessments on the major freight rail crossings over the Western Rivers system in FY 2010.
- **Freight Rail Security Grant Program:** The Freight Rail Security Grant Program (FRSGP) was created in FY 2008 as a component of the Transit Security Grant Program. The FRSGP has supported the development of vulnerability assessments and security awareness and emergency response training for railroad frontline employees. Although the primary grant recipients

have been Class II and Class III railroad carriers, Class I carriers have been eligible for security training funding, provided that they have completed an acceptable vulnerability assessment and security plan. The objective for funding security training is to raise employee security awareness from a basic level to one that is cognizant of carrier company security plans, including IED awareness and related skills.

Improve sector situational awareness, understanding, and collaboration

- **Corporate Security Reviews:** The CSR program is an “instructive” review of a company’s security plan and procedures, and it provides the Federal Government with a general understanding of each company’s ability to protect its critical assets and its methods for protecting hazardous materials under its control. Teams from the Division analyze the railroad’s security plan for sufficiency, determine the degree to which mitigation measures are implemented throughout the company, and recommend additional mitigation measures. The team may also conduct site visits of operations, including critical bridges, tunnels, operations centers, and yards. The company’s critical asset list is also discussed to gain an understanding of its “criticality” determination. Specific mitigation strategies are tied to identified vulnerabilities and are discussed with company officials.
- **Research Projects Related to TIH Rail Transportation:** Currently several projects aimed at gaining a better understanding of the mechanisms and consequences associated with attacks on rail tank cars that transport TIH materials are underway. These projects include:

- **TIH Material (Chlorine) Tank Car Consequence Analysis/Validation**

The project will identify a scientific and computer-based methodology supported by industry, government, and the academic community that can be used to predict the behavior of a catastrophic chlorine release after an attack on a 90-ton DOT Spec 105J500W tank car in a densely populated urban area. Chlorine is a Hazard Zone B TIH material. TSA is leading a project to assess the current dispersion models specific to rail car releases, identify deficiencies in current models, recommend actions that will address those gaps, and develop and execute a program to implement those recommendations. TSA has a need to realistically model large-scale TIH material releases, such as an intentional chlorine release from a railroad tank car, as part of its threat analysis mission. A thorough understanding of the circumstances and effects of past accidental TIH releases is important for assessing existing models and fulfilling the mission. This capability gap is applicable to DHS’s overarching concerns with chemical facility security, TIH tank cars in transport and in temporary storage in rail yards, and emergency response.

- **TIH Material Rail Tank Car Threat Assessment**

The purpose of this project is to identify, define, and prioritize threats and threat scenarios for TIH materials rail tank cars, to evaluate the likely methods of attack an adversary would use to breach a TIH material tank car, and to define the types and amounts of explosives and weaponry placement on the tank car. The results of this project allow for the evaluation of the tank car’s vulnerability to a ballistic attack.

- **TIH Material Rail Tank Car Vulnerability**

The purpose of this program is to better understand and quantify the vulnerability of tank cars used to transport TIH materials to identified terrorist attack methods. Objectives of this project include:

- › Assisting in the development of rail tank car security vulnerability reduction measures; and
- › Estimating the release rate from the breached tank car for emergency response and dispersion modeling purposes.

- **TSA’s Tank Car Vulnerability Assessment Project:** TSA is funding a tank car vulnerability assessment project to better understand the weapons that would likely be used against a TIH tank car and their likely impact on the TIH tank car. With support from a team of experts from DHS, the Federal Bureau of Investigation (FBI), and DoD, the weapon threats against the TIH tank car were identified, defined, and prioritized. An engineering analysis of the weapon’s impact on the TIH tank

car was conducted by the DHS Transportation Security Lab and the Naval Surface Warfare Center (NSWC) which is being followed up with actual tank car weapons impact testing at the Aberdeen Proving Grounds.

- **Next Generation Rail Tank Car Project:** The Dow Chemical Company, in partnership with the Union Tank Car Company and the Union Pacific Railroad, is developing a “Next Generation” rail tank car that will better withstand the destructive forces a tank car may see in a violent train derailment. TSA, through a Memorandum of Cooperation with the Dow Chemical Company, is working to incorporate technologies that can provide protection against high-caliber firearms. DoD components at NSWC Indian Head and NSWC Carderock are providing technical assistance in the development of the Next Generation Tank Car as it relates to protection from the effects of ballistic weapons.
- **Tank Car Hardening Project (aka “Dragon Shield”):** TSA was involved in a government-industry working group consisting of representatives from the Federal Railroad Association (FRA), AAR, the Railway Supply Institute, the American Chemistry Council, the Chlorine Institute, and NSWC Indian Head to examine methods to harden tank cars by providing ballistic penetration resistance and/or self-sealant capabilities. FRA provided funding for this project. Ballistic penetration and self-sealing tests of a series of chlorine tank car plates covered with materials submitted by vendor companies throughout the U.S were conducted at NSWC Dahlgren. The test results provided some promising results with additional testing needed. This built upon tank car vulnerability assessments initiated in 2002 by the freight railroads. This project is complete.
- **Advanced Tank Car Collaborative Research Program (ATCCRP):** Railroad, shipper, and tank car builder groups, with support from TSA, FRA, Transport Canada, and DHS S&T, have collaborated on tank car safety and security research to reduce potential public safety and security risks associated with the transportation of TIH materials. Those groups, represented by the AAR, the American Chemistry Council, the Chlorine Institute, The Fertilizer Institute, and the Railway Supply Institute, agreed to work together on an Advanced Tank Car Collaborative Research Program to promote improvements in rail tank car safety and security. The focus is on the transportation by rail of TIH materials. The ATCCRP is working to identify and characterize promising tank car design concepts and technologies that can be successfully used by tank car builders to achieve significant risk reductions in rail tank car safety and security. This research initiative intends to reduce or eliminate the likelihood of a release of a TIH material from a rail tank car due to an accident or security breach.
- **Understanding Large-Scale Toxic Chemical Transport Releases:** The DHS S&T Chemical Security Analysis Center (CSAC) has been tasked with investigating knowledge and capability gaps that were identified by TSA, in the prediction of the impact and behavior of large-scale TIH material releases. For large-scale releases of tank car quantities of TIH materials, there is insufficient knowledge pertaining to cloud formation, liquid pooling, vaporization rate, the effects of buildings and terrain as well as other factors that are needed to make a proper evaluation and impact prediction. Deficiencies were brought to light after the large scale TIH material releases from rail car accidents in Graniteville, SC (2005) and Macdona, TX (2004) where the released TIH cloud behavior did not match with accepted scientific predictions. Efforts to better understand large TIH releases include conducting a scientific literature gap analysis, a toxicity analysis, and laboratory, wind tunnel and small-scale field tests. Release testing of approximately one ton quantities of chlorine and anhydrous ammonia was conducted in the spring of 2010 at the Dugway Proving Grounds, Utah. The DHS CSAC has acknowledged that large-scale release testing will be required to adequately complete this project.

3.6 Metrics for Continuous Improvement

TIH Risk Reduction Program

In 2007, TSA began assessing the potential vulnerabilities and consequences posed by TIH rail cars in major cities by gathering, monitoring, and quantifying risk information associated with TIH rail shipments traveling through 46 HTUAs. The assessment program was developed to measure the progress Federal and industry efforts are having in reducing the risk associated with the transportation of TIH in major cities. TSA collects and uses both historical and current information on the number of TIH

rail shipments in each HTUA, security at rail yards holding TIH shipments in each HTUA, and the population of each of these cities. Specifically, TSA compiles information for four factors:

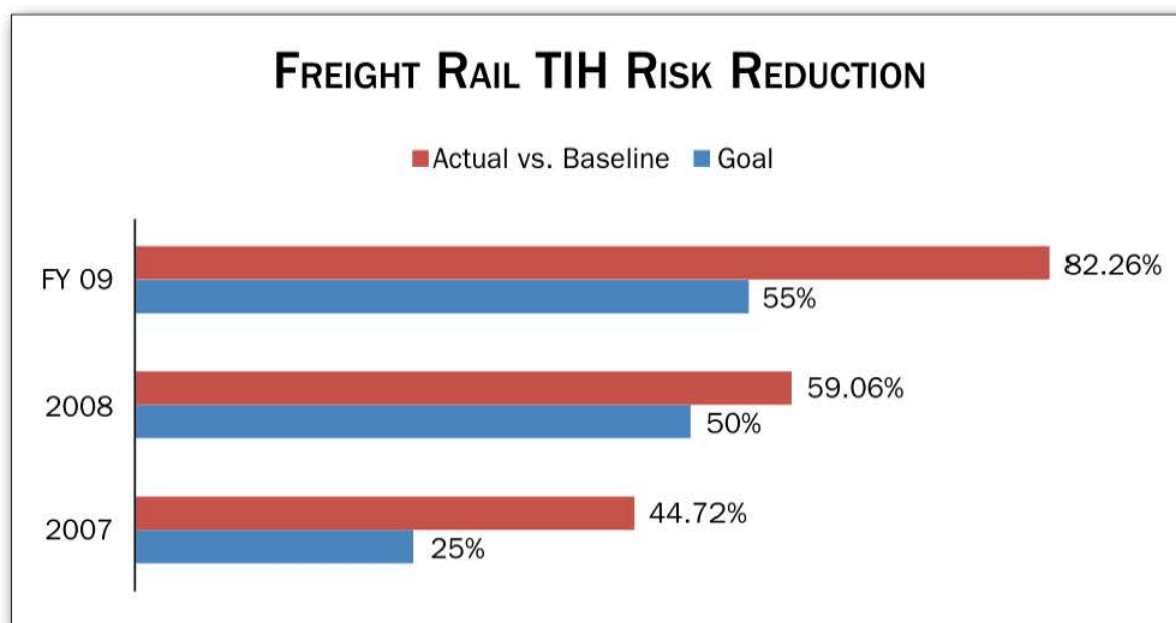
- **Total hours TIH cars were present inside an HTUA.** TSA collects data from the rail industry's automated systems that record the movement and location of all rail cars within the U.S. rail system by means of electronic identification tags. TSA uses these data to quantify the amount of time TIH rail cars are located within a city.
- **Unattended hours of loaded TIH cars inside an HTUA.** TSA collects this information through in-person visits conducted by TSA Transportation Security Inspectors (TSIs).
- **Population proximity to unattended TIH cars.** TSA uses U.S. Census Bureau data to determine the population within a 1-mile radius of each TIH car that was sitting unattended and to rank each city's possible exposure based on this information.
- **City ranking.** TSA prioritizes the cities' importance on a scale of 1 to 5 (5 being the highest) using a logarithmic factor based on the population of each city.

TSA then developed a formula, based on the information collected, to quantify a risk score for each city. The risk score is a relative measure, or indicator, of the TIH security risks within a city for a given time period. Historical information for these risk factors was gathered from June 1, 2005 to May 31, 2006. This information was used to establish a baseline risk score for each of the 46 HTUAs as a means of comparison to the information for the current year.

As of December 2008, TSA determined that there was over a 59 percent national reduction in risk since the end of the baseline period. This achievement surpassed the original goal of a 50 percent risk reduction by the end of 2008. The information TSA has collected gives the agency a way to closely compare the vulnerabilities and consequences related to TIH transportation across various cities over time. The development of national risk scorecards, which ranks each city by risk score, also allows the agency to monitor which cities or railroads have high-risk scores, and to focus further assessment and security efforts on these cities or railroads.

Continued risk reductions will require maintaining the reductions already achieved. This will be accomplished by leveraging TSIs to continue field verification of risk reduction methods, as well as setting a path for achievement of additional reductions in out years. The Office of Management and Budget recognized the significant benefits derived from the TIH Risk Reduction Program, designated the program as a Program Assessment Rating Tool, and tasked TSA with continuing the program through calendar year 2013. TSA continues to measure the ongoing risk associated with the movement of TIH shipments within the same 46 HTUAs. However, in addition to comparing the ongoing risk against the original baseline, each year will also be compared to the prior year, with the goal of a 10 percent risk reduction over the previous year.

Figure E3-2: Freight Rail TIH Risk Reduction



Note on TIH risk reduction baseline measurement: As the baseline period preceded having the TSA surface inspection force in place and as there was an absence of data on the percentage of unattended cars, TSA estimated the percentage using information gathered from assessments performed by the TSA Freight Rail Division and from elicitations with railroad security and operations managers. TSA also established a baseline for population proximity based on geographic center points for the railroad yards with the highest volumes of TIH traffic in the HTUAs. These baseline estimates were used until a full year of data had been collected. Once a full year of collected data was available, TSA began to measure risk reduction on a year-to-year basis using actual field observations rather than estimations of the percentage of attendance and proximity of TIH rail cars to surrounding populations.

The Chain of Custody provisions¹⁸ of the rail transportation security rule also require regulated entities to attend shipments of RSSM, including TIH, to ensure a positive and secure exchange. Requiring covered parties to establish chain of custody and control procedures will further reduce the risk of TIH rail transportation in HTUAs. TSIs will be utilized to monitor rule compliance.

Freight Rail Risk Reduction Metrics

To measure other aspects of security preparedness, the following metrics have been established for the freight rail mode. Measurement of these metrics will commence in FY 2010 by the Division. The corporate security review will serve as the primary method for gathering the necessary data. The measurement results will be prepared on an annual basis and will be shared with the Freight Rail SCC and other industry stakeholders to foster an environment of continuing risk reduction through planning, training, and execution.

¹⁸ 49 CFR 1580.107.

- Vulnerability Assessments – percentage of railroad carriers completing vulnerability assessments that include the identification of critical assets and analysis of asset vulnerabilities.
- Security Plans – percentage of railroad carriers that have system security plans in place that, at a minimum, meet the requirements of 49 CFR 172.802 and address specific security countermeasures for critical asset protection at elevated alert levels.
- Vetting of Employees – percentage of frontline railroad employees that have been vetted through the use of a security threat assessment (e.g., issuance of Transportation Worker Identification Credentials, employer-sponsored background checks).
- Training of Employees – percentage of employees that have been 1) trained in security awareness in accordance with 49 CFR 172.704, and 2) trained in the procedures for the identification and recognition of IEDs in the railroad environment.
- Drills and Exercises – percentage of railroads that have participated in a security-focused exercise within the past 12 months.
- Security Awareness – percentage of railroads that have active employee security awareness programs.
- Screening of Cargo – percentage of trains inbound to the contiguous United States from Canada and Mexico that are screened by Customs and Border Protection.
- Technology Applications – means of measurement to be determined.
- Secure Critical Infrastructure – means of measurement to be determined.

Security Action Item Implementation Surveys: In September 2006, TSA initiated surveys to objectively measure the level of industry implementation of seven field critical action items¹⁹ from the first 24 SAIs. The seven critical action items that were assessed and measured had been selected due to their direct impact on transportation security and because they are most directly tied to practices and procedures applied in the field rather than at the corporate level.²⁰ These surveys were not compliance inspections, but rather assessments to determine the depth and degree of employee security awareness and SAI implementation. During the course of the visit, the inspectors observed conditions in the facility and interviewed frontline employees to determine the level of implementation. TSIs visited railroad yards and terminals in each of the 46 HTUAs from September to December 2006, conducting assessments of over 150 individual railroad facilities, and interviewing over 2,600 employees.²¹

As TSA's summary report on the transportation of TIH materials points out: "In general, the findings from the surveys revealed that the railroads had instituted training programs and implemented procedures to meet the spirit of the security guidelines. Numerically the findings, when averaged across all carriers, showed implementation in the low/medium to medium range. A review of the comments from the TSIs in support of their findings reveals that most railroad employees had a firm understanding of two of the most important guidelines as they directly relate to their duties. These are: 1) awareness of their role and responsibility in operational security, and 2) the signs of suspicious persons or activities at their worksite."²²

The second round of implementation surveys concentrated on the implementation of management policies at field locations and reviewed 10 additional SAIs. These surveys were completed during the second and third quarters of FY 2007. The general level of implementation was good, but there were obvious gaps in the manner in which corporate policies were applied in the field. The surveys also found that the level of knowledge of individual managers varied regarding the security procedures and policies of their companies. The results of both rounds of surveys were provided to the rail carriers surveyed to assist in their efforts to raise the level of security awareness of employees and to set a new baseline for future improvement.

¹⁹ The seven field critical action items included in Phase I of the Security Action Item Implementation Surveys are as follows: (1) employee security awareness; (2) reporting suspicious activity; (3) control of sensitive information; (4) employee identification; (5) systems to locate TIH cars; (6) security focused inspection of TIH cars; and (7) placement of TIH cars in yards.

²⁰ DHS, TSA, TSNM, Freight Rail Security Division. *Freight Rail Transportation of Toxic Inhalation Hazard Materials. Security Action Item Implementation Survey Summary Report 2006*. Washington, D.C. 2006. p. 1.

²¹ Ibid.

²² DHS, TSA, TSNM, Freight Rail Security Division. *Freight Rail Transportation of Toxic Inhalation Hazard Materials. Security Action Item Implementation Survey Summary Report 2006*. Washington, D.C. 2006. p. 1.

4. Security Gaps

Both the Federal Government and private industry stakeholders have undertaken a wide range of actions to measure and reduce the risk to the freight rail system. These efforts have led to a reduction in the risk associated with the transportation of TIH shipments by rail, as well as assessments of a company's ability to protect its critical assets. While these actions have mitigated some of the risk to the freight rail system, vulnerabilities still remain, thus efforts to address them need to continue. A constantly evolving threat environment also creates new security gaps that need to be dealt with. In evaluating the security of the freight rail system, TSA has identified the following gaps which must be addressed in order to protect and secure the Nation's freight rail system.

Reduce the Vulnerability of Cargo

Gap 1.1

Shipments of TIH and other RSSM traveling through HTUAs continue to be vulnerable and pose a risk of catastrophic release if attacked.

Gap 1.2

Certain materials not currently classified as RSSM may have the potential to be used as weapons of mass consequence during transportation. A need exists to specifically assess the potential for these materials to be exploited in the physical state in which they are commonly transported.

Reduce the Vulnerability of the Network

Gap 2.1

Existing Federal training standards do not fully address the knowledge, skills, and abilities required to prepare frontline railroad employees to meet current and emerging security threats. In the 9/11 Commission Act, Congress recognized this gap and required DHS to issue regulations for comprehensive security training programs.

Gap 2.2

While the security planning requirements found in 49 CFR 172.802 provided a framework for vulnerability assessments and security plans, these requirements focus on the security of hazardous materials transportation rather than on the security of the network as a whole. In the 9/11 Commission Act, Congress recognized this regulatory gap and required DHS to issue rules requiring more comprehensive security planning.

Gap 2.3

There is a lack of clear understanding of what is truly critical infrastructure in the freight rail network. A variety of criteria have been applied when ranking or evaluating the criticality of a particular asset. This variance in rating criteria has resulted in inconsistent determination which has led to numerous CIKR lists. These multiple lists do not always mirror each other and could lead to the inefficient deployment of resources, leaving truly critical infrastructure inadequately protected. The Division has developed a critical infrastructure risk assessment tool and plans to seek comment and acceptance from freight rail owners/operators of critical infrastructure. The TSA tool will measure criticality and vulnerability and apply metrics to those elements.

Minimization of Consequences from an Attack

Gap 3.1

Determining the location and tracking of rail cars transporting TIH material in and near HTUAs continues to be a gap, as emergency response and security mitigation efforts are hampered without timely knowledge of TIH rail car locations.

Gap 3.2

In the current state of the emergency response profession, there is a knowledge gap pertaining to the operating procedures for the response to intentionally caused releases of TIH materials, such as chlorine. Emergency response plans and procedures are generally focused on dealing with accidental releases of hazardous materials where the focus is on control and containment of the release and the concurrent protection of nearby populations.

Gap 3.3

Current plume dispersion modeling software applications used to predict the consequences from a catastrophic release of a dense, toxic cloud do not have a sufficient degree of accuracy or scientific agreement to be useful to emergency and security planners. A plume dispersion model that adequately accounts for source terms and real life atmospheric conditions is required.



dated....

5. National Strategy for Freight Rail Transportation Security

Strategic Goal

Reduce the risk associated with the freight rail transportation of potentially dangerous cargoes and increase the resiliency of the freight rail network.

The overall strategic risk objective of the programs in the freight rail mode is to build a safer, more secure, and more resilient freight rail network by enhancing protection of freight rail cargo shipments and critical infrastructure to prevent, deter, neutralize, and mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them. Risk can be viewed as the product of TVC. While it may be impossible to eliminate all threats, the vulnerability of an asset and the consequences of attacking that asset can be mitigated or reduced.

Strategic Methodology

Partner with industry and government stakeholders to identify and implement programs and processes to achieve measurable risk reduction through collaborative and regulatory initiatives.

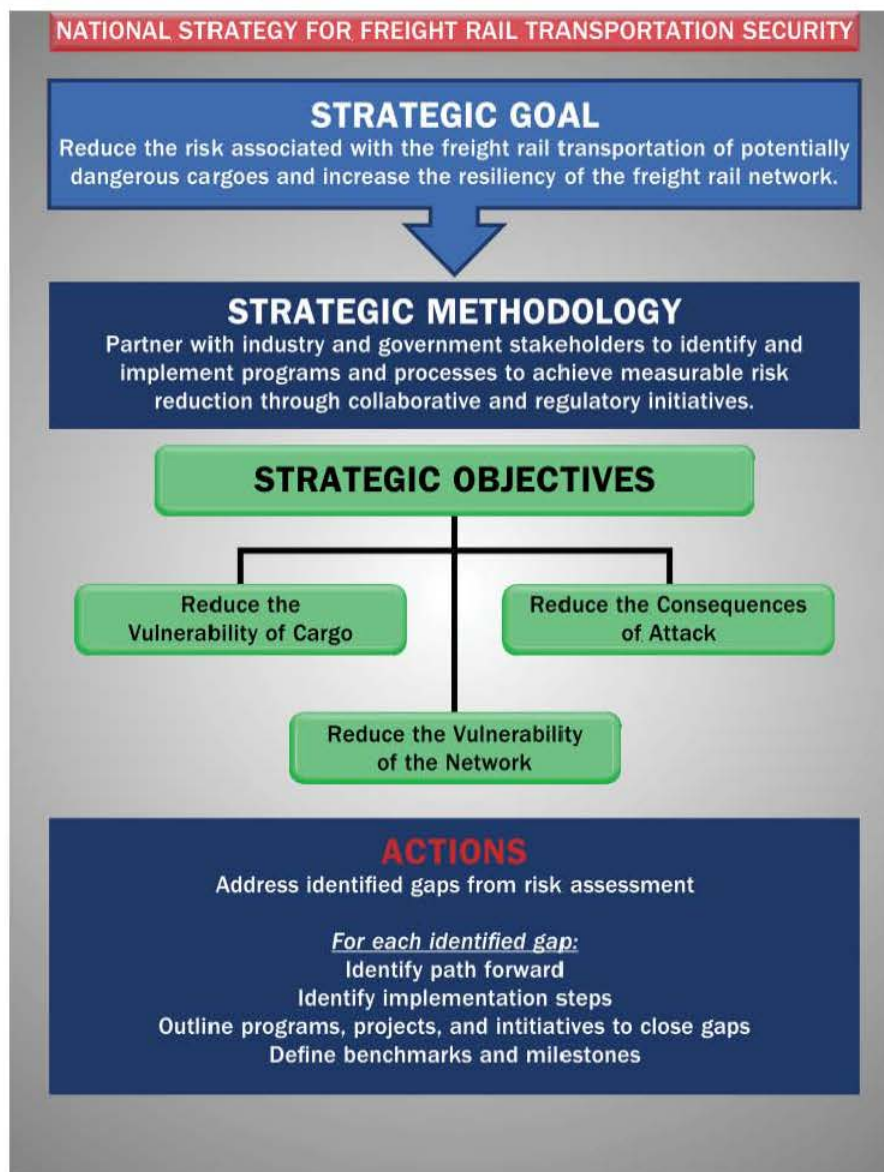
Reducing the risk to cargo and the freight rail network, and minimizing the consequences from an attack, can only be achieved by employing both collaborative and mandatory measures. This approach will allow for the development of layered security measures that will result in the overall reduction of risk. Collaborative initiatives where the industry is a partner in determining implementation steps are necessary to maintain a nimble stance that can react to emerging threats in a timely fashion. Mandatory measures are also necessary to ensure that there is a consistency of implementation that serves as the foundation of layered security.

Strategic Objectives

- **Reduce the vulnerability of cargo**
- **Reduce the vulnerability of the network**
- **Reduce the consequences of attack**

Given the myriad threats and potential vulnerabilities that could be exploited to harm the American public and to hamper the Nation's freight rail network, a clear focus is necessary so that actions can be prioritized and improvements implemented. The three themes that the Division will consider in moving forward will be to: 1) reduce the vulnerability of cargo, 2) reduce the vulnerability of the network, and 3) reduce the consequences of attack.

Figure E5-1: National Strategy for Freight Rail Transportation Security



Reducing the vulnerability of cargo means simply to make it more difficult for adversaries to use potentially dangerous cargoes against the public. A potential threat exists that legitimate cargoes could be intentionally released during transportation causing casualties in nearby populations, damaging infrastructure, and causing disruption in other transportation systems. By making it more difficult for an adversary to target these cargoes and the conveyances that transport them, the overall vulnerability can be reduced. Increased vigilance by those responsible for shipping and carrying these cargoes can also reduce their vulnerability. The following are programs and initiatives that are ongoing or planned to reduce the vulnerability of cargo.

- **Toxic Inhalation Hazard – Risk Reduction Program (TIH-RRP)**

Objective – To objectively measure risk reduction associated with the transportation of TIH materials through HTUAs.

Benchmarks/Milestones – 10 percent reduction each year over previous year.

- **Rail Corridor Comprehensive Reviews (CRs)**

Objectives – Evaluate freight rail operations in HTUAs to identify security control points and recommend mitigation measures to reduce risk; coordinate communication between owners/operators, government, and first responders to bring about enhanced preparedness and domain awareness.

Benchmarks/Milestones – Three reviews each fiscal year.

- **Rail Corridor Assessments (RCAs)**

Objective – Evaluate freight rail operations in HTUAs to identify security control points and recommend mitigation measures to reduce risk.

Benchmarks/Milestones – The surface transportation security inspection force has a target of nine assessments each fiscal year.

- **Best Practices and Security Action Items (SAI) Implementation Surveys**

Objective – To achieve consistent improvement through the adoption and implementation of the security action items by freight railroads.

Benchmarks/Milestones – In FY 2010, TSA will re-evaluate the level of implementation of the security action items in the original 46 HTUAs and will begin a baseline assessment of implementation in the 16 HTUAs that were added in FY 2008.

- **Rail Transportation Security Rule – Final Rule issued November 26, 2008 (73 FR 72130)**

Objective – Address critical vulnerabilities of RSSM transportation through mandatory standards for the positive control and custody of shipments at origin, carrier-to-carrier interchanges, and points of delivery in HTUAs.

Benchmarks/Milestones – Active enforcement commenced in the third quarter of 2009 by TSIs; inspection reports are evaluated at year's end to determine the level of compliance with the regulation.

- **Enhancing Rail Transportation Safety and Security for Hazardous Materials Shipments – Final Rule issued November 26, 2008 (73 FR 72182)**

Objective – Ensure that railroads use routes with the fewest overall safety and security risks to transport RSSM.

Benchmarks/Milestones – Railroads to compile data and information concerning commodities they transport and routes utilized beginning July 1, 2008. Initial risk and route assessments were to be completed by September 1, 2009 (if the railroad used traffic data from July 1 through December 31, 2008), or by March 31, 2010 (if the railroad used traffic data for all of 2008).

- **Tank Car Vulnerability Assessment including Tank Car Hardening Design Efforts**

Objectives – Assist in the development of rail tank car security vulnerability reduction measures. Estimate the release rate from a breached tank car for emergency response and dispersion modeling purposes.

Benchmarks/Milestones – Initial analysis and modeling completed in FY 2008. Field tests to validate analyses were scheduled for FY 2010.

- **Ammonium Nitrate Detonability Study**

Objective – Assess expected outcomes of a terrorist attack on a rail car containing agricultural grade, un-carbonized, ammonium nitrate (AN) (UN 2067) in a highly populated area.

Benchmarks/Milestones – The TSA Explosives Unit, FBI, Technical Security Working Group, and Oak Ridge National Laboratory are conducting a gap analysis to determine the information available from classified and unclassified sources that provide documentation as to the expected detonability of agricultural grade AN. Particular interest is in the AN tests conducted by the Bureau of Alcohol, Tobacco, Firearms and Explosives, and the FBI. Results will be used for decisionmaking regarding explosive materials being transported through HTUAs.

Reducing the vulnerability of the network means to enact processes, procedures, and protections that will reduce the likelihood of a successful attack on freight rail infrastructure. The consequence of an attack on a single location or feature of the freight rail network is not expected to result in widespread impact. However, the anticipated delays and service disruptions that would result do necessitate that measures are taken to increase the probability that the attempted attack is detected and defeated. Protection of critical infrastructure is one of the core programs of homeland security. The following are active initiatives in the freight rail mode.

- **Rulemaking for Enhanced Security Training Standards for Frontline Railroad Employees**

Objective – TSA, during FY 2009, began developing a rulemaking to bring frontline employees to the desired state of knowledge and security awareness by considering craft-specific training situations and security-related regulations.

Benchmarks/Milestones – NPRM in 2011; Final Rule in 2012.

- **Freight Rail Security Grant Program**

Objective – For FY 2010, the FRS GP will make funds available for security training of frontline employees, the completion of vulnerability assessments, the development of security plans within the freight rail industry, and GPS tracking systems for TIH railroad cars.

Benchmarks/Milestones – Applicants are selected through a competitive process based on their ability to deliver training, develop security plans and vulnerability assessments, and proposals to install tracking devices on rail cars carrying TIH.

- **Develop and Issue Rulemaking for Freight Rail Vulnerability Assessments and Security Plans**

Objective – Provide guidance and standards to be utilized in regulatory development for railroads to conduct vulnerability assessments and develop security plans with consideration given to facilities, infrastructure, and protection of shipments; applicability to previous vulnerability assessments; and the ability to build upon existing plans.

Benchmarks/Milestones – NPRM in 2011; Final Rule in 2012.

- **Corporate Security Reviews**

Objective – Conduct an “instructive” review of a carrier’s security plan and procedures that ascertain each freight railroad’s ability to protect its critical assets and its methods for protecting RSSM under its control. Analyze the railroad’s security plan for sufficiency, determine the degree that mitigation measures are implemented throughout the company, and recommend additional mitigation measures. Site visits of operations, including critical bridges, tunnels, operations centers, and yards, can also be conducted. The company’s critical asset list is also discussed to gain an understanding of its “criticality” determination. Specific mitigation strategies are tied to identified vulnerabilities and are discussed with company officials.

Benchmarks/Milestones – Reviews began in 2007. All seven Class I carriers were completed as of October 1, 2007. Review of Class II and III railroads commenced in 2008, and a minimum of four reviews are scheduled for each year. TSA intended to conduct updated reviews of Class I railroads in FY 2010.

- **Integrate and Establish Standard Critical Infrastructure Evaluation Criteria**

Objective – To create a methodology and process that results in national and business critical determinations of critical infrastructure. Consolidate the varying lists being utilized to identify critical rail infrastructure.

Benchmarks/Milestones – FY 2009 – Assembled stakeholder working groups to establish baseline criteria for the evaluation of freight rail assets beginning with bridges. FY 2010 – Conduct in-depth analysis of bridge and tunnel assets.

- **Rail Corridor Comprehensive Reviews**

Objectives – Evaluate freight rail operations in HTUAs to identify security control points and recommend mitigation measures to reduce risk. The comprehensive review will also identify critical infrastructure within the HTUA rail corridors.

Benchmarks/Milestones – Completion of three full reviews each fiscal year.

- **Rail Corridor Assessments**

Objective – Evaluate freight rail operations in HTUAs to identify security control points and recommend mitigation measures to reduce risk.

Benchmarks/Milestones – Nine assessments completed each year by TSIs.

Reducing the consequences of an attack is a core theme of many DHS programs. These range from preparing emergency responders to deal with the results of a large-scale release of a toxic gas, to ensuring that the owners/operators in the freight rail mode have plans in place to address the potential need to re-route traffic or employ countermeasures. The reality that an attack may occur and be successful must be accounted for in preparation and planning initiatives. The programs aimed at increasing the resiliency of the freight rail mode are as follows.

- **Emergency Response to a Catastrophic TIH Material Tank Car Release**

Objective – Reduce the potential consequences of an attack on a TIH material tank car by working with the first responder community to foster enhanced planning and response procedures for catastrophic releases of toxic materials.

Benchmarks/Milestones – Roundtables have been conducted in Los Angeles and Chicago with members of the emergency response community. Additional workshops were scheduled for FY 2010 in conjunction with rail corridor CRs.

- **Tank Car Consequence Analysis and Plume Modeling**

Objective – Identify a scientific, computer-based methodology supported by industry, government, and the academic community. Methodology can then be used to predict the behavior of a catastrophic chlorine release after an attack on a 90-ton DOT Spec 105J500W tank car in a densely populated urban area.

Benchmarks/Milestones – A project team has conducted gap analysis and determined areas in present modeling capabilities that could be the cause of significant discrepancies between modeled and accidental releases. DHS S&T has funded a study of accidental TIH material rail tank car accidents in which large amounts of TIH materials were released, such as in Macdona, Texas in 2004 and Graniteville, South Carolina in 2005. This information will be used to conduct dispersion modeling analysis and validate dispersion modeling results. DHS S&T has provided FY 2009, 2010, and 2011 funding for the project. This is in addition to funds being provided by TSA. TSA will also coordinate its efforts with the Defense Threat Reduction Agency, which has parallel interests in this area.

The National Strategy Crosswalk graphic below lists the freight rail mode's primary security gaps, and identifies the initiatives, programs, and policies to help close those gaps. The strategic objective that each mitigation activity supports is also shown. Many of these mitigation activities are already in operation by TSA and the freight rail industry.

Table E5-2: National Strategy Crosswalk

National Strategy Crosswalk		Strategic Objectives		
		Reduce the Vulnerability of Cargo	Reduce the Vulnerability of the Network	Reduce the Consequences of Attack
Primary Gaps and Initiatives				
1.1	Shipments of RSSM traveling through HTUAs continue to be vulnerable and pose a significant risk if attacked.			
	TIH Risk Reduction Program	X		
	Comprehensive Reviews	X		
	Rail Corridor Assessments	X		
	Security Action Items and Implementation Surveys	X		
	Rail Transportation Security Rule (49 CFR Parts 1520 and 1580)	X		
	Enhancing Rail Transportation Safety and Security for Hazardous Materials Shipments - Final Rule issued November 26, 2008 (73 FR 72182)	X		
1.2	A need exists to fully understand and quantify the vulnerability of tank cars used to transport TIH materials to terrorist attack.			
	Tank car vulnerability assessment including tank car hardening design efforts	X		
1.3	As not all hazardous materials are currently classified as RSSM, a need exists to assess the potential for these materials to be exploited in the physical state in which they are commonly transported.			
	Ammonium Nitrate Detonability Study	X		
2.1	Existing training standards do not adequately address the knowledge, skills, and abilities required to ensure frontline railroad employees are prepared to meet current and emerging security threats.			

	TSA draft rulemaking for frontline rail employee training standards		X	
	Freight Rail Security Grant Program		X	
2.2	Security planning requirements found in 49 CFR 172.802 provide a framework for vulnerability assessments and security plans. These requirements focus on the security of hazardous materials transportation rather than on the security of the network as a whole.			
	Develop and issue rulemaking for Freight Rail Security Plans		X	
	Develop Vulnerability Assessment Completion rulemaking		X	
	Corporate Security Reviews (CSR)		X	
2.3	There is currently a divergence of opinions on what constitutes CIKR within the freight rail network. This variance in rating criteria has resulted in inconsistent determinations leading to a multitude of CIKR.			
	Integrate and establish standard critical infrastructure evaluation criteria		X	
	Comprehensive Reviews		X	
	Rail Corridor Assessments		X	
3.1	Currently there is not a national coordinated system for tracking and locating rail cars loaded with TIH materials. Without timely knowledge of the RSSM cars in and near HTUAs, emergency response and security protections may be delayed.			
	Freight Rail Security Grant Programs to promote equipping TIH tank cars with GPS tracking systems			X
	Reporting of location and shipping information (49 CFR 1580.103)			X
3.2	In the current state of the profession, there is a knowledge gap pertaining to the operating procedures for the response to intentionally caused releases of TIH materials, such as chlorine.			
	Develop guidelines for emergency response planning for a catastrophic release of toxic materials			X



Annex F: Pipeline



Contents

1. Executive Summary	315
2. Pipeline Overview	317
2.1. Pipeline Mode Description	317
2.2. Assets, Systems and Networks	317
2.3. Risk Profile (Threats to Pipelines)	318
2.4. Sector Partners and Information Sharing Mechanisms	319
2.4.1. Federal Agencies Responsible for Pipelines	319
2.4.2. Information Sharing	319
3. Implementation Plan	321
3.1. Goals, Objectives, and Programs/Projects/Activities	321
3.1.1. Transportation Systems Sector Goals	321
3.1.2. Pipeline Modal Objectives	322
3.1.3. Pipeline Modal Supporting Strategies	322
3.2. Strategic Risk	323
3.3. Operational Risk	323
3.4. Decisionmaking Factors	324
3.5. Risk Mitigation Pipeline Activities, Programs, and Projects	325
3.5.1. TSA-Led Programs, Projects, and Activities	325
3.5.3. Pipeline Industry-Led Programs, Projects, and Activities	328
3.5.4. Industry Smart Practices, Guidelines, Standards, and Programs	329
3.6. Metrics	329
4. Security Gaps	331
5. Way Forward	333
Appendix 1. Objectives/ Strategies/ Programs/ Goals Alignment Table	335

List of Figures

Figure F2-1: Oil and Gas Movement to Market	318
Figure F3-1: Goals, Objectives, and Strategies Alignment	321
Figure F3-2: Risk Definition Framework	324



1. Executive Summary

Each day, thousands of businesses and millions of people rely on the safe, secure, and efficient movement of commodities through the transportation system. Manmade or natural disruptions to this critical system could result in significant harm to the social and economic well-being of the country. The Nation's pipeline system is a mode of transportation with unique infrastructure security characteristics and requirements.

As required by Executive Order 13416,¹ the Pipeline Modal Annex implements the Transportation Systems Sector-Specific Plan (SSP) and was developed to ensure the security and resiliency of the pipeline mode.

The vision of this plan is to ensure that the pipeline mode is secure, resilient, and able to quickly detect physical and cyber intrusions or attacks, mitigate the adverse consequences of an incident, and quickly restore pipeline service. A robust nationwide pipeline security program will instill public confidence in the reliability of the Nation's critical energy infrastructure, enhance public safety, and ensure the continued functioning of other critical infrastructure sectors that depend on secure and reliable supplies of products for consumption.

The SSP and the Pipeline Modal Annex were developed, reviewed, and updated using both the Transportation Systems Sector and the Energy Sector Government Coordinating Council (GCC) and Sector Coordinating Council (SCC) frameworks. The draft plans were distributed to the pipeline industry via the GCC and SCC memberships for another level of review and input before finalizing the documents.

The Transportation Security Administration (TSA) Pipeline Security Division will work with its security partners in both the Transportation Systems and Energy Sectors to update the Transportation Systems SSP and Pipeline Modal Annex regularly, as called for in the National Infrastructure Protection Plan (NIPP) and Executive Order 13416. The updating process is a responsibility shared with pipeline partners collaboratively through the GCC/SCC/Critical Infrastructure Partnership Advisory Council (CIPAC) framework.

The core of the plan is the TSA pipeline system relative risk assessment and prioritization methodology. This methodology provides a logical prioritization process to systematically list, analyze, and sort pipeline systems. By prioritization, security resources can be effectively used to manage risk mitigation in order to protect critical pipelines from threats. The methodology is based on the Transportation Systems Sector Risk Management Framework methodology, which is, in turn, based on the risk management framework presented in the NIPP.

¹ Strengthening Surface Transportation Security, December 5, 2006.

With a view toward this future-state, the SSP and this Pipeline Modal Annex specifically focus on how the Pipeline Security Division within the Transportation Systems Sector will continue to enhance the security of its critical infrastructure and key resources (CIKR).

The Pipeline Security programs developed to protect the Nation's pipeline system(s) are key to making the nation safer, more secure, and more resilient in the face of all hazards.

2. Pipeline Overview

2.1 Pipeline Mode Description

The Nation's pipeline system is a mode of transportation with unique infrastructure security characteristics and requirements. Vast networks of pipelines traverse hundreds of thousands of miles to transport nearly all of the natural gas and about 65 percent of hazardous liquids, including crude and refined petroleum products, consumed within the United States. Pipelines are an efficient and fundamentally safe means of transportation. However, pipelines also transport hydrocarbons that can potentially cause deaths and injuries to the general public, and/or inflict damage to the environment. Most pipelines are privately owned and operated, and with rare exceptions, are buried underground. The pipeline industry's current security posture is based on voluntary guidelines that were developed, issued, and implemented through a collaborative effort between the Federal government and industry associations.

2.2 Assets, Systems and Networks

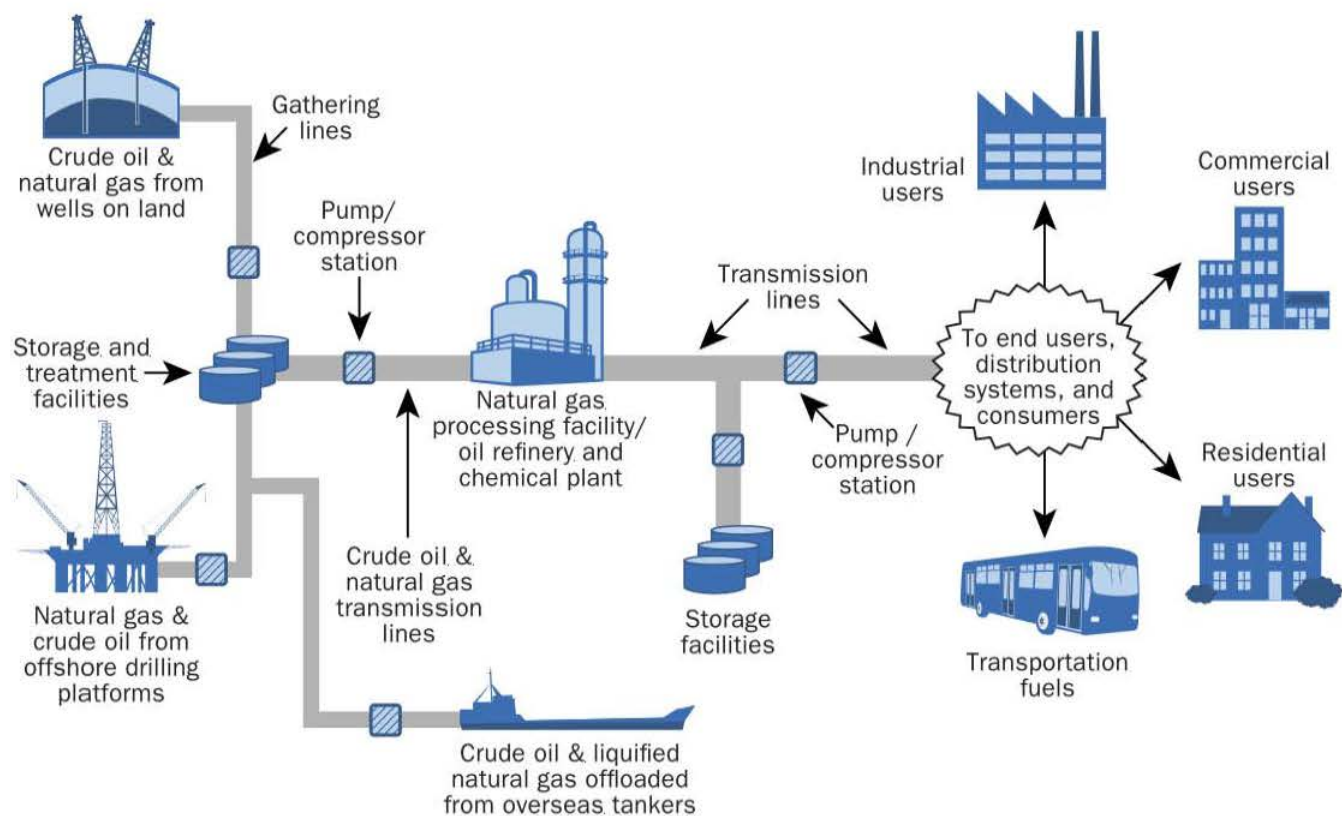
The following are the main types of pipelines:²

1. **Natural Gas Transmission and Storage.** These lines are mostly interstate, transporting natural gas over 320,500 miles of pipelines from sources to communities, operated by more than 700 operators. More than 400 natural gas storage facilities are in the United States.
2. **Hazardous Liquid Pipelines and Tanks.** These pipelines predominately consist of interstate pipelines transporting crude oil to refineries and refined petroleum products (e.g., fuels) to marketing terminals and airports; they carry diesel fuel, gasoline, jet fuel, anhydrous ammonia, and carbon dioxide to product terminals and airports. Nationwide, there are about 168,900 miles of these pipelines in operation, operated by more than 200 operators.
3. **Natural Gas Distribution.** These are typically local distribution company pipelines, mostly intrastate, that transport natural gas from transmission pipelines to residential, commercial, and industrial customers. Included in this segment of the industry are the local distribution companies, i.e., natural gas utilities. More than 1,300 operators operate approximately 2.2 million miles of natural gas distribution pipelines nationwide.
4. **Liquefied Natural Gas (LNG) Processing and Storage Facilities.** More than 109 facilities nationwide either directly receive LNG from tanks, ships, or trucks, or receive natural gas via pipeline for processing (liquefying) into LNG and then store it on site in specialized tanks. When needed, LNG is vaporized for injection into natural gas pipeline systems.

² The following sources were used for information in this section: DOT Bureau of Transportation Statistics; DOT Office of Pipeline Safety; Association of Oil Pipelines; American Gas Association; American Public Gas Association; and Interstate Natural Gas Association of America.

Figure F2-1 shows the structure of oil and gas pipeline system movement to market.

Figure F2-1: Oil and Gas Movement to Market



2.3 Risk Profile (Threats to Pipelines)

The pipeline system is a vital part of the U.S. transportation and energy supply, with connections to other critical infrastructure such as airports and power plants. Since the attacks of September 11, 2001, numerous federal warnings have been issued specifically mentioning pipelines as terrorist targets. Many pipelines carry volatile and flammable materials that have the potential to cause serious injury to the public and the environment. The pipeline system is uniquely vulnerable to terrorist attacks because of the products transported, and because pipeline networks are widely dispersed across both remote and urban portions of the country. A pipeline facility could be vandalized or attacked with explosive devices, resulting in flow disruption or the release of its contents.

Pipelines are also susceptible to cyber attacks on their computer control systems. Cyber threats could result from the acts of a terrorist-hacker, or a rogue employee with computer access. The latter threat requires that specific attention be given to personnel security credentials and access protocols, as well as general cybersecurity protocols. Additionally, attacks on other infrastructure such as regional electricity grids and communication networks could cause a serious disruption in pipeline operations, posing risks for all sectors serviced by pipelines, including the military and major commercial installations.

It is impossible to uniformly protect the pipeline system. While it is difficult to predict what method of attack may be utilized, the risks can be calculated in terms of threat, vulnerability, and consequence, and measures can be taken to safeguard the pipeline system.

American oil pipelines carry over 75 percent of the Nation's crude oil and 60 percent of its refined petroleum products.³ A majority of the Nation's natural gas moves from well to market via pipeline. In addition to oil and natural gas transmission, pipelines are used to transport manufacturing chemicals such as anhydrous ammonia, a critical fertilizer for the American farming industry and feedstock for the chemical industry.

Pipeline disruptions can have effects that ripple through the economy, and at the most extreme, can impact public health and national security. Minor disruptions may result in increased prices of gasoline, diesel fuel, home heating oil, and natural gas. More prolonged disruptions could manifest themselves as widespread energy shortages and the inability to produce products such as plastics, pharmaceuticals, and many chemicals that rely on oil and natural gas as manufacturing feedstock. In the case of an extreme disruption of pipelines, American transportation and manufacturing could be halted, homes could go cold for lack of natural gas or heating oil, and energy for vital defense use may begin to limit American defense capabilities.

2.4 Sector Partners and Information-Sharing Mechanisms

Each of the transportation modes is required to have a GCC. A Pipeline Working Group has been established to address pipeline issues within the Energy Sector GCC. To avoid duplication and eliminate the need for multiple meetings with the same security partners, the Energy Sector GCC Pipeline Working Group also acts as the Pipeline GCC for the Transportation Systems Sector GCC.

The Oil and Natural Gas (ONG) SCC has also established a Pipeline Working Group to address pipelines issues. The ONG SCC Pipeline Working Group also acts as the Pipeline SCC for the Transportation Systems SCC.

The TSA Pipeline Security Division has been a member of the Energy Sector GCC since its inception, and the Department of Energy (DOE) is a member of the Transportation Systems Sector GCC as well. More details on the Energy Sector GCC and ONG SCC can be found in the Energy SSP.

2.4.1 Federal Agencies Responsible for Pipelines

Under the NIPP, TSA is assigned as a Sector-Specific Agency (SSA) for the Transportation Systems Sector, including the pipeline systems mode. The United States Coast Guard is the SSA for the Transportation Systems Sector maritime mode. SSAs are responsible for coordinating infrastructure protection activities within the critical infrastructure sectors. DOE is the SSA for the Energy Sector and therefore works closely with TSA on pipeline security issues, programs, and activities. The Department of Transportation (DOT) is responsible for administering a national program of safety in natural gas and hazardous liquid pipeline transportation, and TSA and DOT collaborate on matters relating to transportation security and transportation infrastructure protection. The Department of Justice through the Federal Bureau of Investigation (FBI) is responsible for investigating and prosecuting actual or attempted attacks on, sabotage of, or disruptions of critical infrastructure in collaboration with the Department of Homeland Security (DHS).

2.4.2 Information Sharing

A number of methods have been employed and will continue to be used to foster good communication and information sharing within the pipeline mode.

³ Bureau of Transportation Statistics (BTS), "National Transportation Statistics," February 2008.

GCC/SCC/CIPAC Framework

The GCC/SCC/CIPAC framework has been and will continue to be used to facilitate discussion and information sharing among pipeline security partners.

TSA Pipeline Security Stakeholder Conference Calls

Since March 2006, the TSA Pipeline Security Division has conducted regular conference calls with pipeline security partners. These conference calls are used to share pipeline security information and educate security partners on many of the programs, activities, and initiatives within the pipeline mode or within the Transportation Systems Sector. These conference calls also provide pipeline security partners with the opportunity to ask questions and bring up other important issues for discussion. Ad-hoc stakeholder conference calls can be conducted on short notice as the need arises.

Trade Associations

As appropriate, information is also disseminated through five major trade associations with strong ties to the pipeline industry:

- American Petroleum Institute (API),
- Association of Oil Pipe Lines (AOPL),
- American Public Gas Association (APGA),
- Interstate Natural Gas Association of America (INGAA), and
- American Gas Association (AGA).

These associations can quickly pass information to their member companies, as demonstrated by the numerous information-sharing sessions through conference calls they have conducted with their respective security committees over the past eight years.

Homeland Security Information Network

The Homeland Security Information Network (HSIN) is an Internet-based communications system DHS established to facilitate exchanging information between DHS and other government, private sector, and non-governmental organizations involved in counterterrorism and incident management activities. In May 2006, the ONG SCC signed a Memorandum of Understanding (MOU) with DHS to establish the ONG HSIN. The TSA Pipeline Security Division communications and information-sharing activities have been incorporated into the ONG HSIN system. There is a link to the TSA Transportation Security Information Sharing and Analysis Center (TS-ISAC) on the ONG HSIN system. Pipeline information can also be found on the TS-ISAC network.

TSA Transportation Suspicious Incident Report

TSA's Office of Intelligence disseminates the Transportation Suspicious Incident Report (TSIR), a weekly unclassified report on all suspicious activity related to transportation. The TSIR includes incident reporting, analyses, images, and graphics on transportation security activities. In addition, select articles focus on security technologies, terrorism, and the challenges of securing the Nation's transportation modes. TSA's Pipeline Security Division shares this weekly report with all interested pipeline security partners in an effort to maintain government transparency and to enhance and improve incident communication and sharing.

Federal Energy Regulatory Commission Pipeline Engineering Data and Damage Reporting

The Federal Energy Regulatory Commission (FERC) has taken steps to provide relevant engineering data that it receives from jurisdictional interstate pipelines in the context of facility siting and permitting to the DOE. In June 2006, the FERC also revised its regulations to require jurisdictional pipelines to report major damage to pipeline systems that result from major disasters, whether they are natural (such as a hurricane) or manmade (such as a terrorist attack). This revision was made, in part, to enhance its ability to provide relevant information to GCC and SCC activities.

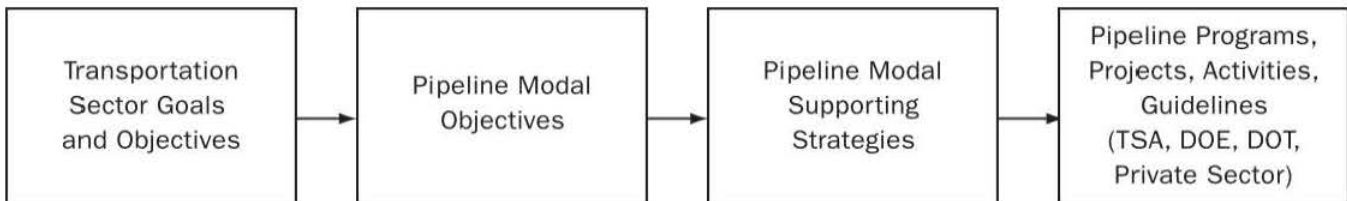
3. Implementation Plan

3.1 Goals, Objectives, and Programs/Projects/Activities

Four overarching Transportation Systems Sector goals and 17 supporting objectives are consistent with the goals outlined in the President’s homeland security agenda, DHS priorities, and the statutory imperatives for protecting the transportation system and improving resiliency of its critical infrastructure and networks (chapter 1, section 1.3 of the Transportation Systems SSP). The Pipeline Modal Annex outlines three objectives that aim to achieve the sector goals within the pipeline transportation domain. Each pipeline modal objective is achieved by a combination of one or more of seven underlying modal strategies. Each of these seven modal strategies is, in turn, supported by programs, projects, and activities. These programs, projects, and activities are the result of the combined contributions of the TSA Pipeline Security Division and other Federal, State, local, and private sector partners and reflect the significant efforts of all pipeline stakeholders to secure our Nation’s pipeline systems.

Figure F3-1 shows the relationships between all goals, objectives, programs, projects, and activities. The sector goals and objectives are supported by the modal objectives; the modal objectives are supported by the strategies, and so on.

Figure F3-1: Goals, Objectives, and Strategies Alignment



The following subsections define the sector goals and objectives, the modal objectives, their supporting strategies, and the programs, projects, and activities. The tables at the end of section 3 provide a specific, detailed description of each modal objective; the strategies, programs, projects, and activities that support it; and the sector goals to which it aligns.

3.1.1 Transportation Systems Sector Goals

The following are the Transportation Systems Sector’s overarching goals:

- Goal 1: Prevent and deter acts of terrorism using, or against, the transportation system.**
- Goal 2: Enhance the all-hazard preparedness and resilience of the global transportation system to safeguard U.S. national interests.**

Goal 3: Improve the effective use of resources for transportation security.

Goal 4: Improve sector situational awareness, understanding, and collaboration.

3.1.2 Pipeline Modal Objectives

The three objectives for the Pipeline Modal Annex are as follows:

1. **Reduce level of risk through analysis and implementation of security programs** that enhance deterrence and mitigate critical infrastructure vulnerabilities against threats and natural hazards.
2. **Increase the level of resiliency and robustness** of pipeline systems and operations through collaborative implementation of measures that increase response preparedness capabilities and minimize effects caused by attack from threats or natural hazards.
3. **Increase the level of domain awareness, information sharing, response planning, and coordination** through enhanced training, network building, and efficient research and development application.

While no specific objective is directed at achieving “cost-effective use of resources,” where possible each strategy involves maximizing efficient employment of available resources and minimizing duplication of effort. The sector objectives will thereby be supported through the conscious efforts of all stakeholders to make evaluations of cost versus risk and to maximize the use of already available resources.

3.1.3 Pipeline Modal Supporting Strategies

Each modal objective is achieved through a combination of strategies. Each strategy is directly supported by a combination of programs, projects, or activities. These strategies are further described here. The programs, projects, and activities are listed below, along with a brief description and the function and corresponding strategies they support. The following are the modal strategies:

1. Promote the implementation of layered threat deterrence and vulnerability mitigation programs in pipeline systems and critical infrastructure, considering risk analysis and making efficient use of existing resources and minimizing duplication of effort.
2. Develop and perform collaborative risk analysis processes from which mitigation measures and plans are determined using available resources with maximum efficiency.
3. Use collaborative plan development and drill/exercise participation to enhance response, restoration, and recovery capabilities while maximizing efficient use of existing resources and minimizing duplication of effort.
4. Promote pipeline system resiliency and contingency capability enhancement measures that increase pipeline system robustness and resiliency while maximizing efficient use of resources and minimizing duplication of effort.
5. Conduct security-related training that enhances domain awareness of deterrence and mitigation measures, increases knowledge of response and restores capabilities, and clarifies the roles and responsibilities of all stakeholders within the pipeline domain.
6. Conduct network enhancement and information-sharing activities that promote domain awareness, collaborative planning, and the definition of roles and responsibilities for pipeline security partners.
7. Conduct research and development and other activities that build domain awareness in all facets of risk mitigation and resiliency enhancement through coordinated and efficient use of assets.

3.2 Strategic Risk

This section explains how the pipeline mode participates in data collection for risk assessment.

The TSA Pipeline Security Division gathers data by conducting pipeline Corporate Security Reviews (CSRs) and Critical Facility Inspections (CFIs) in cooperation with sector security partners to further evaluate and categorize pipeline systems.

The CSR program has gathered excellent pipeline system data since its conception in 2003. The CSR program is an on-site security review process with pipeline companies that is used to help establish working relationships with key security representatives. CSRs give TSA an understanding of the pipeline operator's security plan and its implementation. The CSR process uses a standard protocol to capture data on pipeline systems, which can be evaluated both quantitatively and qualitatively to further prioritize critical pipeline systems.

During the CSR process, potentially critical assets are examined and catalogued based on their importance to the pipeline systems. Assets are identified and a link between the asset and the critical pipeline system is then documented. Critical assets include pipeline components, such as the following:

- Pipeline interconnections
- Hubs or market centers
- Metering stations
- Pump stations
- Compressor stations, terminals
- Operation control facilities
- Pipeline bridge crossings
- Critical aboveground piping
- Storage facilities

On August 3, 2007, President Bush signed The Implementing Recommendations of the 9/11 Commission Act of 2007, P.L. 110-53 (2007) (9/11 Act). Section 1557 of the law requires TSA, along with DOT, to develop and implement a plan for inspecting the critical facilities of the 100 most critical pipeline systems. The Pipeline Security Division began inspecting the critical facilities in November 2008 and the results of these inspections are used in the data collection process.

3.3 Operational Risk

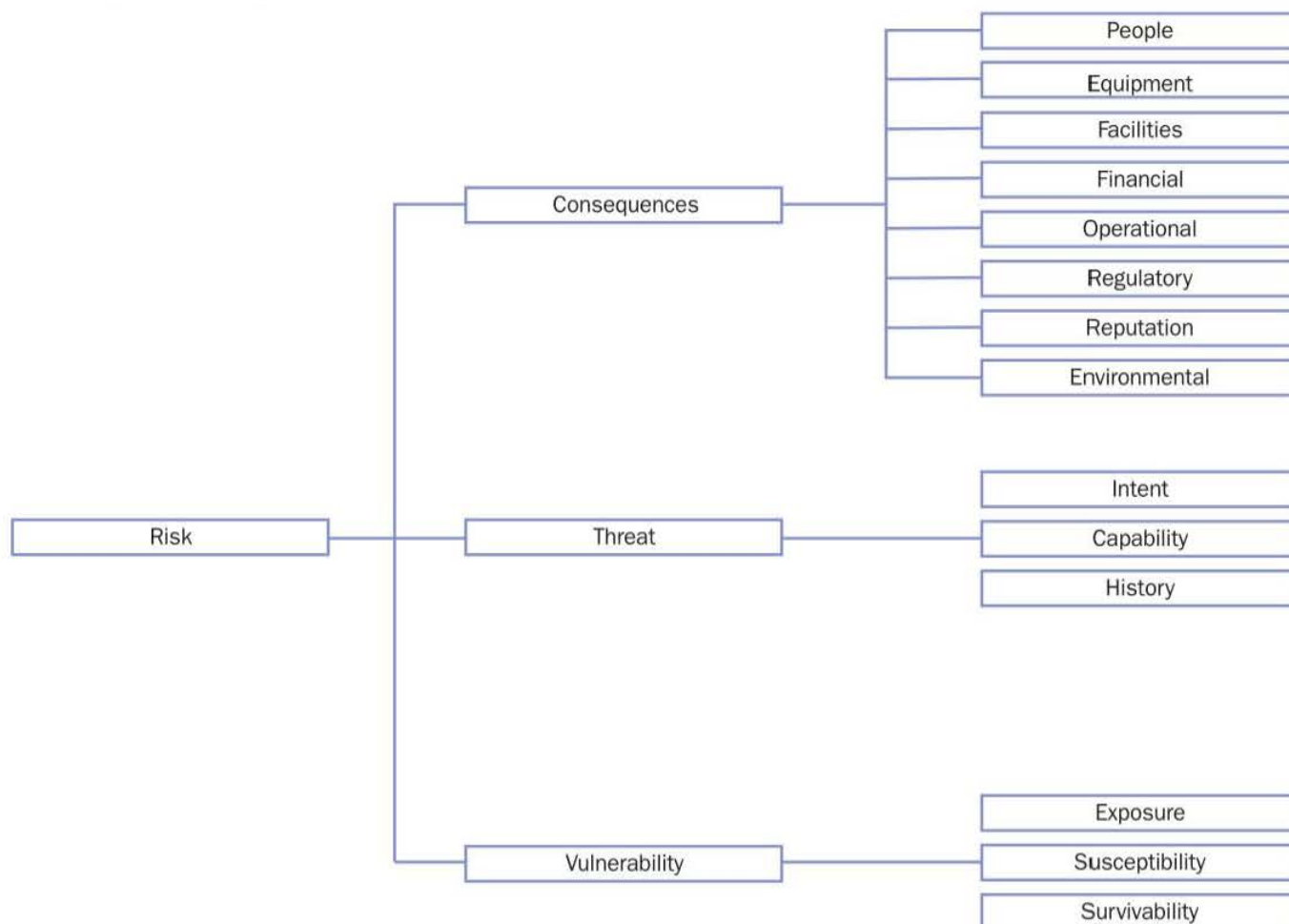
This section explains the pipeline risk assessment method that the TSA Pipeline Security Division utilizes.

In practical terms, a risk-based approach to security is recognizing that there are too many risk scenarios to protect all assets/pipeline/systems equally, so priorities must be established and security resources allocated accordingly. A more theoretical description of risk is that it is a function of likelihood (mathematically expressed as a probability) and consequences (in terms of impact to people or facilities, financial loss, operational disruption, etc.). Likelihood can be further broken down into threat (an adversary's capability and intent) and vulnerability (a target's exposure, susceptibility, survivability).

Measuring risk is a matter of attempting to quantify the various components of it (see above). Some things are, by nature, speculative. For example, one can infer an adversary's intent but not read his or her mind. One must try to measure the various parts of risk for which information is available and make some judgment calls where it is not.

Figure F3-2 shows the framework that will be used to define risk for the purposes of this approach.

Figure F3-2: Risk Definition Framework



Adapted from Patrick Gallagher
Manager, Group Security Intelligence & Risk, Qantas

The TSA Pipeline Security Division relies on TSA's Office of Intelligence to provide threat assessments based on information received from the Intelligence Community: the FBI, Central Intelligence Agency, DHS Office of Intelligence and Analysis, and others.

The TSA Pipeline Security Division uses the results of the CSRs and the CFIs, the pipeline's energy throughput, and the threat as indicators of the security risk in the pipeline industry measured by the formula $R = f(T, V, C)$. The measurable risk is the difference between the desired state and the current state using the Pipeline CSR results (V), the energy throughput (C), and the threat (T).

3.4 Decisionmaking Factors

This section explains the TSA Pipeline Security Division's methods for identifying pipeline modal priorities utilizing the results from the CSRs, the CFIs, and other applicable information.

The natural gas and hazardous liquids pipeline system infrastructure is substantial, widely dispersed, and mostly privately-owned. While there is a desire to secure all aspects of all critical infrastructure, the total pipeline system cannot be given equal oversight, protection, focus, or security resources. Therefore, appropriate resources must be focused where they are needed the most.

A Pipeline System Relative Risk Ranking Tool that provides a logical prioritization process is required to list systematically, analyze, and sort pipeline systems and critical pipeline components within those pipeline systems. The TSA Pipeline Security Division will implement the prioritization process with input from pipeline operators and industry trade associations. Through prioritization, security resources can be used effectively for risk management to protect critical pipelines from all hazards. Pipeline systems will always be ranked and evaluated first before any specific asset or component. The overall guidance for the methodology is introduced in chapter 3 of the Transportation Systems SSP.

Individual pipeline companies conduct security risk analyses on their corporate assets. Reasonable resources should be allocated as necessary to ensure an appropriate level of security. During the CSR process, the TSA Pipeline Security Division will verify that the company's risk analysis is being conducted and reasonable actions taken.

In the first step, the TSA Pipeline Security Division will use quantitative methods to sort and provide a rough screening of more than 2,200 pipeline systems throughout the United States. Hazardous liquids, natural gas distribution, and transmission systems will be sorted by the total equivalent energy transported, typically converted to therms per year. The higher the throughput in therms (i.e., energy delivered to end users), the higher the pipeline system will be sorted on the list. The logic is that systems with higher annual energy shipment are more valuable to the Nation's energy security. In this manner, the total universe of pipeline systems will be pared down to a small finite number for further evaluation in the next steps. Qualitative methods from subject matter experts will also be used where applicable to consider the criticality of certain systems that quantitative methods do not adequately address.

TSA will use the Pipeline System Relative Risk Ranking Tool to rank the most critical systems and assets according to the greatest importance to energy supplies and risk, in threat, vulnerability, and consequences. The list will be sorted using proven qualitative and quantitative methods. A subject matter ranking factor (percentage adding to 100 percent) will weigh the importance on the highest areas of concern.

Using the methodology described above, the algorithm will generate a unit-less relative risk score. The higher the score, the higher the pipeline will be in the relative risk ranking. The algorithm will factor in countermeasures as a negative number, reducing the risk score. With periodic reevaluation, the ranking will probably change over time. In addition, subject matter experts will use their knowledge to verify the algorithm's results.

3.5 Risk Mitigation Pipeline Activities, Programs, and Projects

The tables in sections 3.5.1, 3.5.2, and 3.5.3 present the programs, projects, and activities (either already undertaken or planned) that promote prevention, deterrence, preparedness, system resiliency, and information for physical, human, and cyber threats within the pipeline system domain. Moreover, many programs strengthen partnerships and build security networks that extend internationally as well. These sections are divided into TSA-led efforts, efforts led by other Federal agencies or departments, and pipeline industry initiatives. The tables list the programs, provide a brief description of each, list the participating organizations, and note the pipeline modal strategies each program supports.

3.5.1 TSA-Led Programs, Projects, and Activities

The TSA Pipeline Security Division has numerous programs, projects, and activities designed to increase the security of the Nation's pipeline systems. The cornerstones of these programs are the Pipeline System Relative Risk Ranking and Prioritization Tool and the Pipeline CSR programs.

Program/Project/ Activity	Description	Participants	Pipeline Strategies Supported
Pipeline System Relative Risk Tool	This program and associated activities compile statistical data from CSRs, CFIs, and other data sources on pipeline systems to perform a relative risk ranking.	TSA, Industry	2, 7
Pipeline CSR Program	Since 2003, TSA has been conducting CSRs, an on-site security review, with pipeline companies to help establish working relationships with key security representatives in the pipeline industry as well as provide TSA with a general understanding of a pipeline operator's security planning and implementation.	TSA, Industry	1, 6
Pipeline CFI Program	On August 3, 2007, President Bush signed the 9/11 Act. Section 1557 of the law requires TSA, along with DOT, to develop and implement a plan for inspecting the critical facilities of the 100 most critical pipeline systems. The Pipeline Security Division began inspecting the critical facilities in November 2008.	TSA, Industry	1, 6
Revision of the Pipeline Security Guidelines	In 2002, DOT's Office of Pipeline Safety issued pipeline security guidelines to improve the security posture of the pipeline industry. TSA has widely accepted these guidelines and conducts CSRs of pipeline operators based on these guidelines. After the DOT guidelines were published, TSA was designated in the NIPP as the SSA responsible for pipeline security. As such, the responsibility for revising the guidelines lies with TSA. TSA is in the final process of updating those guidelines, with input from government and industry partners.	TSA, Other Government Agencies, Industry	1,2,3,4,5,6
Pipeline Security Incident and Recovery Protocol Plan	In the 9/11 Act, Section 1558 tasked the Secretary of Homeland Security (TSA) and the Secretary of the DOT Pipeline Hazardous Materials Safety Administration (PHMSA) to develop a Pipeline Security and Incident Recovery Plan and to submit that plan to Congress. The Pipeline Security Division, in collaboration with PHMSA, government and industry partners has completed the plan.	TSA, Other Government Agencies, Industry	1,2,3,4,5,6
TIH Materials Transmitted in Pipelines	In addition to oil and natural gas, pipelines are also used to transmit hazardous materials. This program will address the potential risks associated to the transport of these materials.	TSA, Government Partners, Industry	1,3,5,7
Pipeline Cross- Border Vulnerability Assessment Program (International)	The pipeline cross-border vulnerability assessments are in support of the Smart Border Accord and the Security and Prosperity Partnership Agreement. Assessment teams of Canadian and U.S. subject matter experts in pipeline operations, control systems, infrastructure interdependencies, and assault planning visit critical cross-border pipeline infrastructure, identify security gaps, and recommend protective measures to mitigate those gaps.	TSA, Natural Resources Canada	1, 2, 5

Program/Project/ Activity	Description	Participants	Pipeline Strategies Supported
International Pipeline Security Forum	International forum for U.S. and Canadian Governments and industry pipeline officials to discuss security issues and topics.	TSA, Natural Resources Canada, Government Agencies, Industry	5, 6
Pipeline Exercises, The Intermodal Security Training Exercise Program (I-STEP)	The I-STEP program promoting security partner awareness and involvement, encourages security partner participation in program development, ensures program alignment with national standards and requirements, conducts exercises relevant to security partners' challenges and risks and refines the program through evaluation and continuous improvement.	TSA, Government Partners, Industry	1,2,3,4,5,6,7
Training Materials	Informational CDs about pipeline security issues and improvised explosive devices (IED).	TSA	1, 2, 6
TSA Pipeline Security Stakeholder Conference Calls	Periodic information-sharing teleconference calls between TSA, other government agencies, and industry security partners.	TSA, Other Government Agencies, Industry	6
Transportation Systems GCC, Energy GCC and CIPAC Joint Sector Committee	Government security partners participate in GCCs and CIPAC to coordinate interagency and cross-jurisdictional implementation of security for critical infrastructure.	TSA, DOE, Government Agencies, Industry	6
Pipeline Security Smart Practices	Document to assist hazardous liquid and natural gas pipeline industries in their security planning and implementation.	TSA, Industry	1,4
Homeland Security Information Network (HSIN)	Internet-based communications system and information-sharing tool providing security information, threat intelligence, indications, and warnings.	DHS, TSA, DOE, Industry	6
Homeland Security Advisory System (HSAS)	Information-sharing program that makes government, the private sector, and the public more vigilant when credible threat is identified.	DHS	1, 6
DOT, DOE, DHS Incident Drill Programs/ Sponsorship and Participation	Tabletop and field exercise facilitation.	DOT, DOE, DHS, PHMSA	3, 4

3.5.3 Pipeline Industry-Led Programs, Projects, and Activities

The pipeline industry has been effective in its prevention, deterrence, preparedness, system resiliency, and information-sharing efforts. The following examples are a small sample of the industry's programs, projects, and activities that support the pipeline modal objectives.

Program/Project/ Activity	Description	Participants	Pipeline Strategies Supported
ONG/Pipeline SCC and CIPAC Joint Sector Committee	Private-sector companies participate in the SCC and CIPAC to engage with industry and government security partners in critical infrastructure protection discussions and activities.	Industry, Government Agencies	6
Pipeline Company-Based Drill/Exercise Initiatives and Participation	Private-sector companies participate in drills/exercises related to infrastructure security at all levels (Federal, State, regional, local, and corporate); companies have engaged in tabletop and on-site simulated exercises.	Pipeline Companies	3
Pipeline Company-Based Training Initiatives	Training initiatives include corporate and field training and usually include response measures tied to the DHS Threat Advisory System; tools include briefings, manuals, CDs, and computer-based training.	Pipeline Companies	5
API/NPRA Security Vulnerability Assessment for the Petroleum and Petrochemical Industries	Provides practical knowledge for performing security vulnerability assessments in multiple petroleum and petrochemical-related industries.	API, NPRA	2
API Security Committee and AGA Security Committee-Sponsored Training and Workshops	Workshops/forums and training for gas and liquid petroleum industry.	API	5, 6
Pipeline Company Security Protective and Deterrence Measures	Pipeline operators enhance protective and deterrence measures in accordance with Pipeline Security Circular 2002.	Pipeline Companies	1

3.5.4 Industry Smart Practices, Guidelines, Standards, and Programs

Practices/ Guidelines/ Standards/Program	Description	Participants	Pipeline Strategies Supported
Security Guidelines; Natural Gas Industry, Transmission and Distribution: Assessment Guidelines	Provide an approach for vulnerability assessment, critical facility definition, detection/deterrence methods, response and recovery, cybersecurity, and relevant operational standards.	AGA, INGAA, and APGA	1
Cryptographic Protection of Supervisory Control and Data Acquisition (SCADA) Communications	Define encryption methods for SCADA systems.	AGA	1
API Security in the Petroleum Industry: Practices Guidelines	Recommend security practices for all segments of liquid and gas petroleum.	API	2
API Pipeline SCADA Security Standard (API Standard 1164)	Provide a model for proactive industry actions to improve the security of the Nation's energy infrastructure.	API	1
API Information Management and Technology Program	Provide a comprehensive review and quantitative assessment of company security programs.	API	2

3.6 Metrics

To quantify and establish a pipeline risk reduction metric, the TSA Pipeline Security Division uses the results of the CSRs and the CFIs, the pipeline's energy throughput, and the threat as indicators of the security risk in the pipeline industry measured by the formula $R = f(T, V, C)$. The measurable risk is the difference between the desired state and the current state using the Pipeline CSR results (V), the energy throughput (C), and (T).



4. Security Gaps

The TSA Pipeline Security Division has conducted CSRs since 2003 and began conducting CFIs in 2008. Utilizing the data obtained in those programs and other data resources, the following security gaps and risk mitigation activities and programs have been developed or are under development.

1. Cross-border (international) pipelines are becoming increasingly important to the Nation's pipeline industry. Action Item 21 of the Smart Border Accord requires that the United States and Canada conduct joint assessments on trans-border infrastructure and identify necessary additional protective measures. In the area of pipeline security, TSA has partnered with Natural Resources Canada to conduct system assessments. Six pipeline systems have been reviewed by a joint U.S./Canadian team. The assessments will continue with Canada.
2. Security awareness training is inconsistent throughout the pipeline industry. To address this gap, one of the programs and objectives of the TSA Pipeline Security Division is the development of training CDs and other training materials. The objective of this project is to assist the pipeline industry in achieving desired levels of security through increased knowledge of effective security measures and heightened awareness of vulnerabilities, potential threats, and targets.
3. In addition to oil and natural gas, pipelines are also used to transmit TIH materials. These pipelines have proven to be potential threats and the products present a serious hazard if released. This program will address the potential risks associated to these pipelines and assist the operators with the development of security programs.
4. Security drills and exercise programs are also inconsistent throughout the pipeline industry. To address these gaps, the TSA Pipeline Security Program is developing a pipeline security exercise program in coordination with the pipeline industry and the TSA I-STEP. The I-STEP program promotes security partner awareness and involvement, encourages security partner participation in program development, ensures program alignment with national standards and requirements, conducts exercises relevant to security partners' challenges and risks, and refines the program through evaluation and continuous improvement.

Also, the TSA Pipeline Security Program is coordinating with the Visible Intermodal Prevention and Response (VIPR) teams. VIPR teams are comprised of a variety of personnel drawn from TSA's Federal Air Marshal Service (FAMS), Transportation Security Inspectors, as well as state and local law enforcement (among others). The actual team composition for each VIPR operation is determined collectively by the participating organizations as part of the process of developing a deployment operations plan.

VIPRs, when randomly deployed, can serve as a deterrent, providing a highly visible law enforcement presence at critical pipeline facilities. VIPR operations can disrupt a potential attacker's planning process and give the impression that a facility is too well-protected to be attacked, forcing an attacker to shift his focus elsewhere. In the case of a specific threat to a pipeline facility or system, deploying VIPR teams to protect critical facilities can be a valuable tool to defend key assets. In the case of unmanned facilities, VIPR operations can be conducted covertly, in a counter-surveillance effort. This approach

can be particularly useful if there is a specific threat but the authorities do not want to disclose to the attacker that they have been discovered.

5. In 2002, DOT's Office of Pipeline Safety issued pipeline security guidelines to improve the security posture of the pipeline industry. TSA has widely accepted these guidelines and conducts CSRs of pipeline operators based on these guidelines. After the DOT guidelines were published, TSA was designated in the NIPP as the SSA responsible for pipeline security. TSA, in coordination and collaboration with government and industry partners is in the process of updating the guidelines.
6. The "Pipeline Security Smart Practices" reflect the application of data collected from CSRs conducted since the inception of the program in the fall of 2003. A qualitative and quantitative examination of this data, coupled with literature research of pipeline security measures, identified smart practices operators can institute to promote an effective security program. The practices cover a range of topical security areas, including risk and vulnerability assessments, security planning, threat information, employment screening, facility access controls, physical security, intrusion detection, monitoring systems, SCADA and information technology security, awareness training, incident management planning, drills and exercises, and cooperation with regional and local partners, such as law enforcement and other pipeline operators.
7. In recognition of the need to effectively communicate information pertaining to pipeline incidents, and to synchronize a response among the relevant federal agencies, DHS/TSA and DOT/PHMSA established the Interagency Threat Coordination Committee (ITCC) during the development of the Pipeline Incident and Recovery Plan. The ITCC is designed to organize and communicate developing threat information among federal agencies that may have responsibilities during a pipeline incident response. The ITCC will communicate information at the headquarters level, so the development of Federal action plans can be implemented in a coordinated fashion while avoiding overlap or a duplication of effort. The ITCC will also work to identify any type of assistance that may be useful to owners/operators and provide subject matter information from Federal experts concerning the threat.

5. Way Forward

The TSA Pipeline Security Division will continue to participate in all aforementioned programs, projects, and activities. In addition, the TSA Pipeline Security Division plans to address needed improvements and gaps in the following areas to improve security awareness.

In-Depth Pipeline Assessments – TSA plans to conduct more detailed system and asset assessment programs. Private pipeline operators will have the chance to review and provide input to these assessment programs as well. It is also recommended that pipeline operators conduct detailed system assessments of their critical pipeline systems. In this advanced assessment, TSA and pipeline operators will first assess in greater detail the pipeline systems. The assessment evaluates vulnerabilities and develops mitigation options and countermeasures. Vulnerabilities are the characteristics of a network's, system's, or asset's design, location, security posture, process, or operation that render it susceptible to destruction, incapacitation, or exploitation by mechanical failures, natural hazards, terrorist attacks, or other malicious acts.

The system assessment will evaluate physical security, operations, and processes in a more detailed way than is possible with the current CSR program. Pipeline systems will be evaluated based on how many other operators serve their market areas and on their operational integrity, redundancy, and resilience to attack. The assessment will also examine the impacts of prolonged system downtime and the operator's ability to repair and recover from an attack. The economic and environmental consequences of a system failure will be projected. An operator's corporate security, continuity of operations, disaster recovery plans, and mutual aid arrangements will be evaluated in detail. TSA will assess an operator's ability to recover rapidly, based on supply chain, material, equipment, and manpower resources. TSA will assess the supplies of the commodities the pipeline transported and the availability of alternate sources of supply, the availability of emergency storage, and delivery capabilities. The operator's control processes and control center will be evaluated, as well as cybersecurity for SCADA systems. Communications and management control systems and interdependency with other suppliers and utilities will also be evaluated.

In the future, TSA will assess in greater detail the pipeline assets. The main types of assessments will be facilitated, Federal-led assessments and/or owner-operator self-assessments. In either case, assessors will evaluate existing security measures, vulnerabilities, consequences, and threats. Currently, no single assessment methodology is universally applicable to all system components or assets. A wide variety of tools are currently in use and each varies in assessment approach. As outlined in the NIPP, flexibility on the approaches taken is given as long as it conforms to the NIPP's basic criteria.

Pipeline Security Training – As noted in the Security Gaps section, security awareness training is inconsistent throughout the pipeline industry. To address this gap, one of the programs and objectives of the TSA Pipeline Security Division is the development of training CDs and other training materials. The objective of this project is to assist the pipeline industry in achieving desired levels of security through increased knowledge of effective security measures and heightened awareness of vulnerabilities, potential threats, and targets. TSA has developed a 30-minute training DVD that is tailored specifically to an audience

of pipeline operators. The training covers topics such as security measures, awareness of vulnerabilities, potential threats, and targeting. A second training CD addresses the IED threat to pipelines.

Pipeline Transmission of Hazardous Materials – As noted in the Security Gaps section, pipelines are also used to transmit TIH materials. These pipelines have proven to be potential threats as the products present a serious hazard if released. This program will address the potential risks associated with these pipelines and assist the operators with the development of security programs. Plans are to expand this program in FY 2011 with the addition of resources to the Pipeline Security Division.

Security Drills and Exercises – The TSA Pipeline Security Division is developing a pipeline security exercise program in coordination with the pipeline industry, the TSA I-STEP and the TSA VIPR teams. The first exercise was conducted in October 2009 and the plan is to conduct at least two exercises per year.

Pipeline Security Guidelines and Regulations – The TSA Pipeline Security Division in coordination and collaboration with government and industry partners updated the pipeline security guidelines and planned to issue these guidelines in FY 2010. Section 1557 of the 9/11 Act notes that, if it is determined that regulations are appropriate to reduce risk and apply appropriate mitigation procedures, regulations shall be promulgated and necessary inspection and enforcement actions be developed.

Pipeline Incident Recovery Plan – In the 9/11 Act, Section 1558 of the Act tasked the Secretary of Homeland Security (TSA) and the Secretary of the Department of Transportation (PHMSA) to develop a Pipeline Security and Incident Recovery Plan and to submit that plan to Congress. The Pipeline Security Division in cooperation with PHMSA, government and industry partners has completed the plan and submitted the plan to Congress.⁴

⁴ A copy of the plan can be found at http://www.tsa.gov/what_we_do/tsnm/pipelines/resources.shtml.

Appendix 1. Objectives/ Strategies/ Programs/ Goals Alignment Table

Pipeline Modal Objectives	Supporting Strategies	Supporting Programs, Projects, Activities, Guidelines, etc.	SSP Goals Supported
1. Reduce level of risk through analysis and implementation of security programs that enhance deterrence and mitigate critical infrastructure vulnerabilities against threats and natural disasters.	1. Implement layered threat deterrence and vulnerability mitigation programs	<ul style="list-style-type: none"> • Pipeline Cross Border Vulnerability Assessment Program • Pipeline Corporate Security Review (CSR) Program • CFI Program • Security Awareness Training CD • Pipeline Security Smart Practices • Pipeline Transmission of TIH Materials 	1. Prevent and deter acts of terrorism using, or against, the transportation system. 2. Enhance the all-hazard preparedness and resilience of the global transportation system to safeguard U.S. national interests. 3. Improve the effective use of resources for transportation security. 4. Improve sector situational awareness, understanding, and collaboration.
	2. Develop and perform collaborative risk analysis processes	<ul style="list-style-type: none"> • Pipeline Cross-Border Vulnerability Assessment Program • Pipeline System Relative Risk Tool 	
2. Increase the level of resiliency and robustness of pipeline systems and operations through collaborative implementation of measures that increase response preparedness capabilities and minimize effects caused by attack from threats or from natural disasters.	3. Use collaborative plan development and drill/ exercise participation	<ul style="list-style-type: none"> • Company Based Drill/Exercises Participation • TSA Drills and Exercises • Pipeline Security Incident and Recovery Plan 	1. Prevent and deter acts of terrorism using, or against, the transportation system. 2. Enhance the all-hazard preparedness and resilience of the global transportation system to safeguard U.S. national interests. 3. Improve the effective use of resources for transportation security. 4. Improve sector situational awareness, understanding, and collaboration.
	4. Promote pipeline system resilience and contingency capability enhancement measures	<ul style="list-style-type: none"> • Company Based Drill/Exercises Participation • TSA Drills and Exercises • Pipeline Security Incident and Recovery Plan • Pipeline Policy and Planning 	
	5. Conduct security-related training that enhances domain awareness	<ul style="list-style-type: none"> • TSA Pipeline Security Training Programs 	

Pipeline Modal Objectives	Supporting Strategies	Supporting Programs, Projects, Activities, Guidelines, etc.	SSP Goals Supported
3. Increase the level of domain awareness, information-sharing, and response planning and coordination through enhanced training, network building, and efficient research, development application.	5. Conduct security-related training that enhances domain awareness	<ul style="list-style-type: none"> • DOT-sponsored Contingency, Resiliency, Response, Restore Training/Workshops • TSA Pipeline Security Awareness Training CD • API/AGA Workshops 	<ol style="list-style-type: none"> 1. Prevent and deter acts of terrorism using, or against, the transportation system. 2. Enhance the all-hazard preparedness and resilience of the global transportation system to safeguard U.S. national interests. 3. Improve the effective use of resources for transportation security. 4. Improve sector situational awareness, understanding, and collaboration.
	6. Conduct network enhancement and information-sharing activities	<ul style="list-style-type: none"> • Pipeline Cross Border Vulnerability Assessment Program • CSR Program • CFI Program • International Pipeline Security Forum • Pipeline Policy and Planning • Security Awareness Training CDs • Pipeline Security Smart Practices • TSA Pipeline Security Stakeholder Conference Calls • Pipeline Company-Based Security Training Initiatives 	
	7. Conduct research and development and other activities that build domain awareness	<ul style="list-style-type: none"> • Relative Risk Ranking Tool 	





Homeland
Security

Transportation Systems Sector-Specific Plan 2010