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

List of Figures

List of Tables

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).

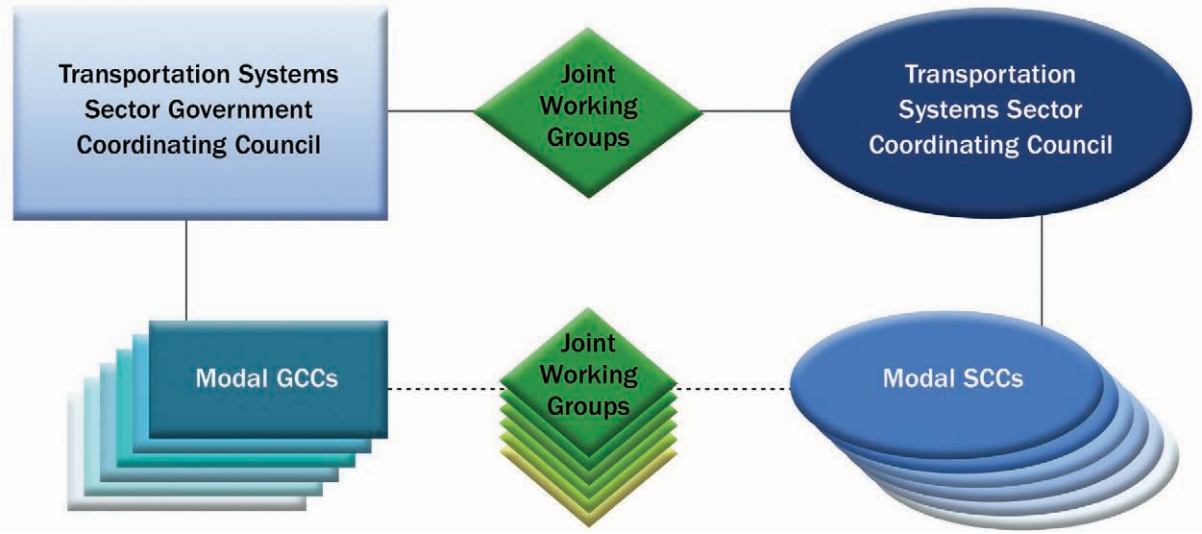
millions of tons of goods each year, makes it a highly attractive target for terrorists, as well as vulnerable to all types of man-made and natural disasters.

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



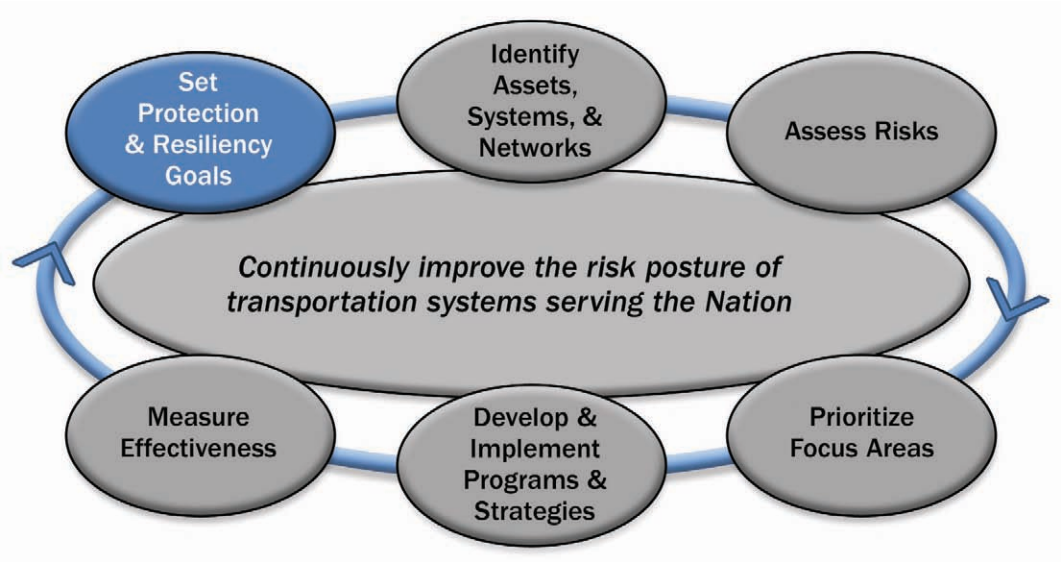
International partnerships are essential to achieve the transportation protection and resiliency objectives. TSA, the USCG, and the Department of State strive to assure that foreign governments and foreign air carriers and transportation companies meet international security protocols and that international 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.

Risk = *f* (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:

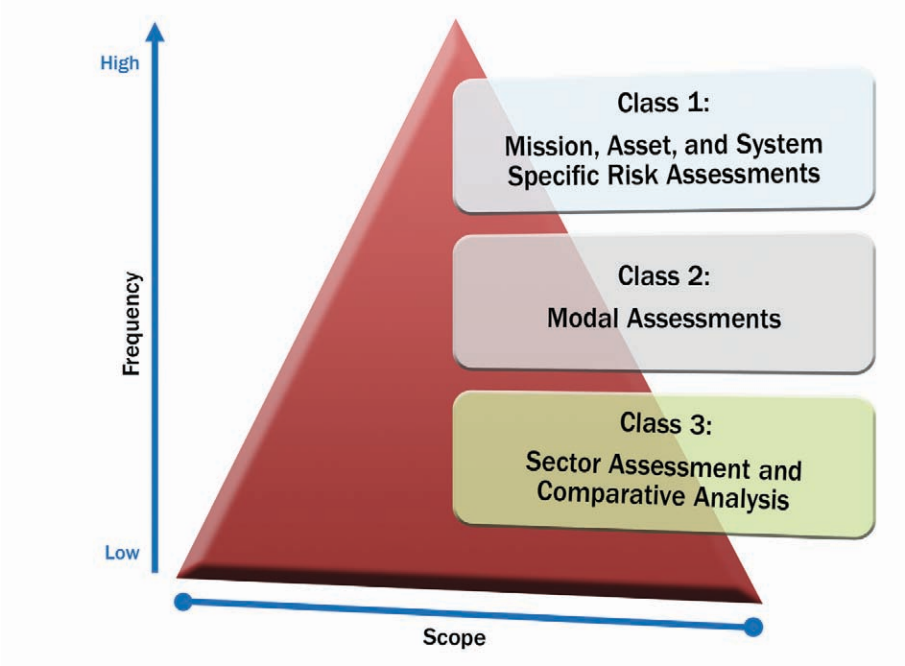
Risk = *f* (Threat, Vulnerability, Consequence) -

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.

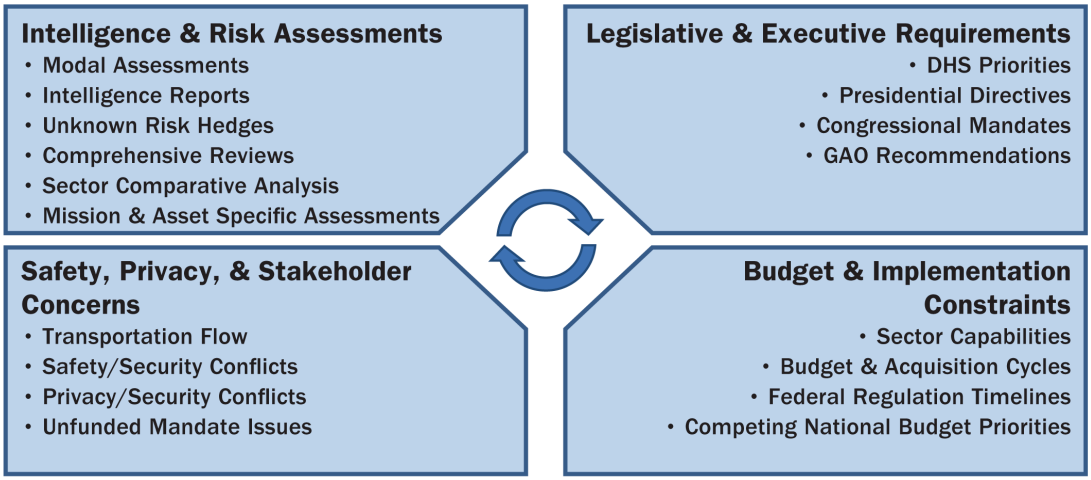
Class 3 assessments are cross-modal comparative analyses focusing on two or more modes, or on the entire sector. These analyses help identify strategic planning priorities and define long-term visions. Cross-modal analyses inform key leadership decisions and policies, including investments in countermeasures.

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 resilience 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	✓	✓		✓

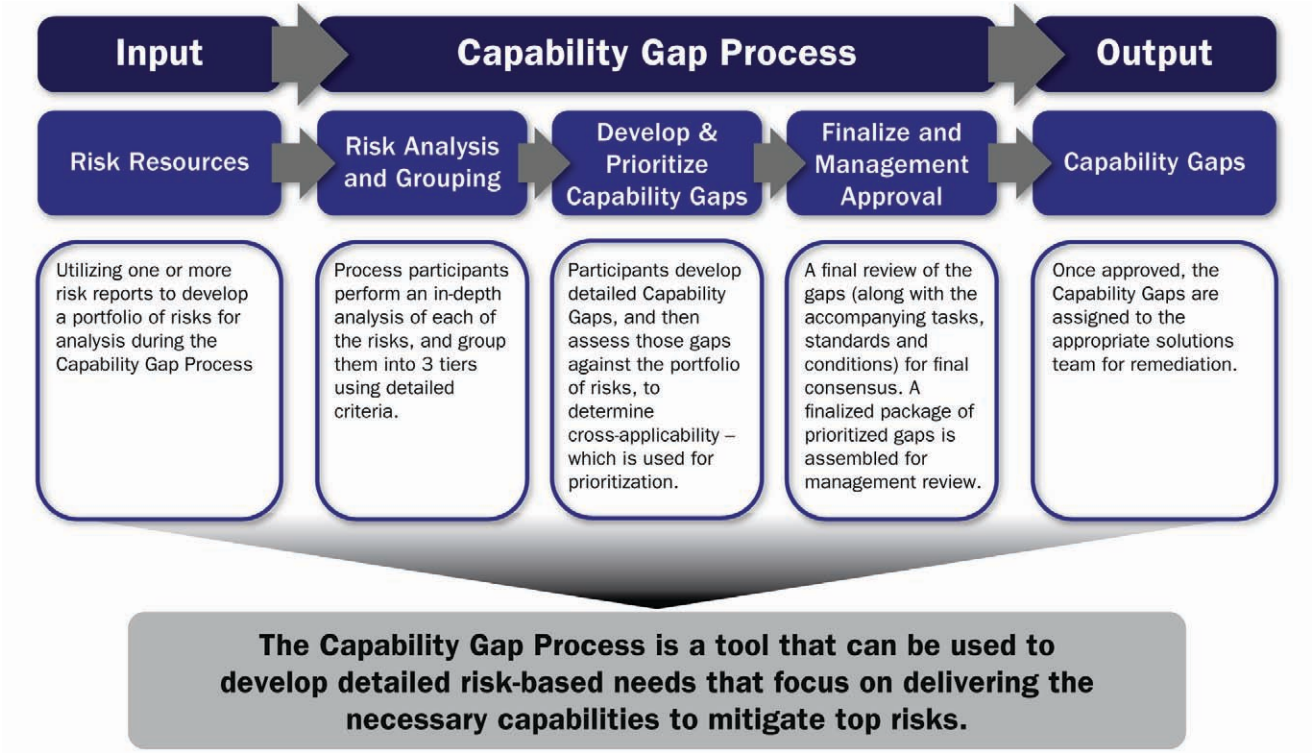
Key Maritime SSA RMA	Goal to which Activity Maps			
	Goal 1	Goal 2	Goal 3	Goal 4
Maritime Domain Awareness	✓	✓	✓	✓
Risk reduction tools and methods	✓	✓	✓	✓
Create and oversee an effective maritime security regime	✓	✓	✓	✓
Lead and conduct effective maritime and security response operations	✓	✓	✓	✓

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:

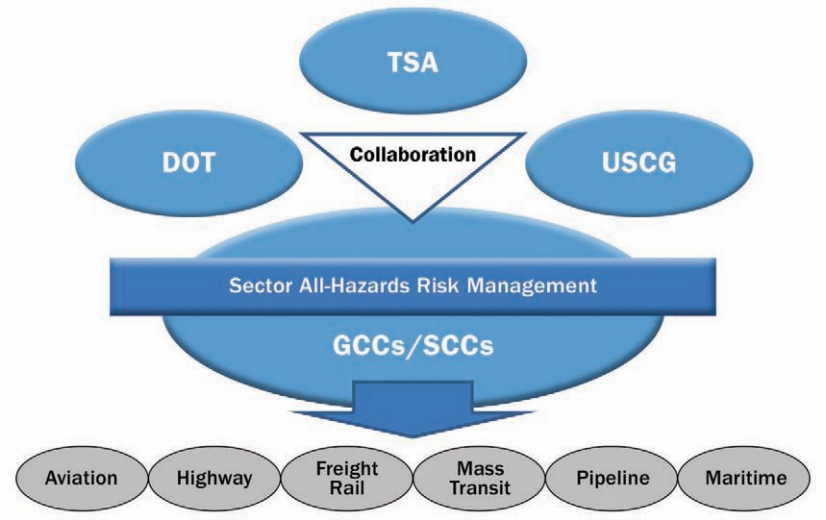
- Enhance screening effectiveness for passengers, baggage, cargo, and materials for the six modes of transportation within the sector;
- Enhance infrastructure and conveyance security;
- Improve information gathering and analysis;

- 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	• Conduct annual review and validation/update based on process feedback • Update modal cybersecurity objectives for modal specific and intermodal concerns
	• 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	• Participate in annual DHS National Critical Infrastructure Prioritization Program and the Critical Foreign Dependencies Initiative
	• 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	• Refine the sector strategic risk assessment model for the annual risk assessment requirement
	• 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	• Update priorities based on annual assessments
	• 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	• 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
	• 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	• Work with government partners and DHS IP to meet the NIPP's annual metrics milestones
	• 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

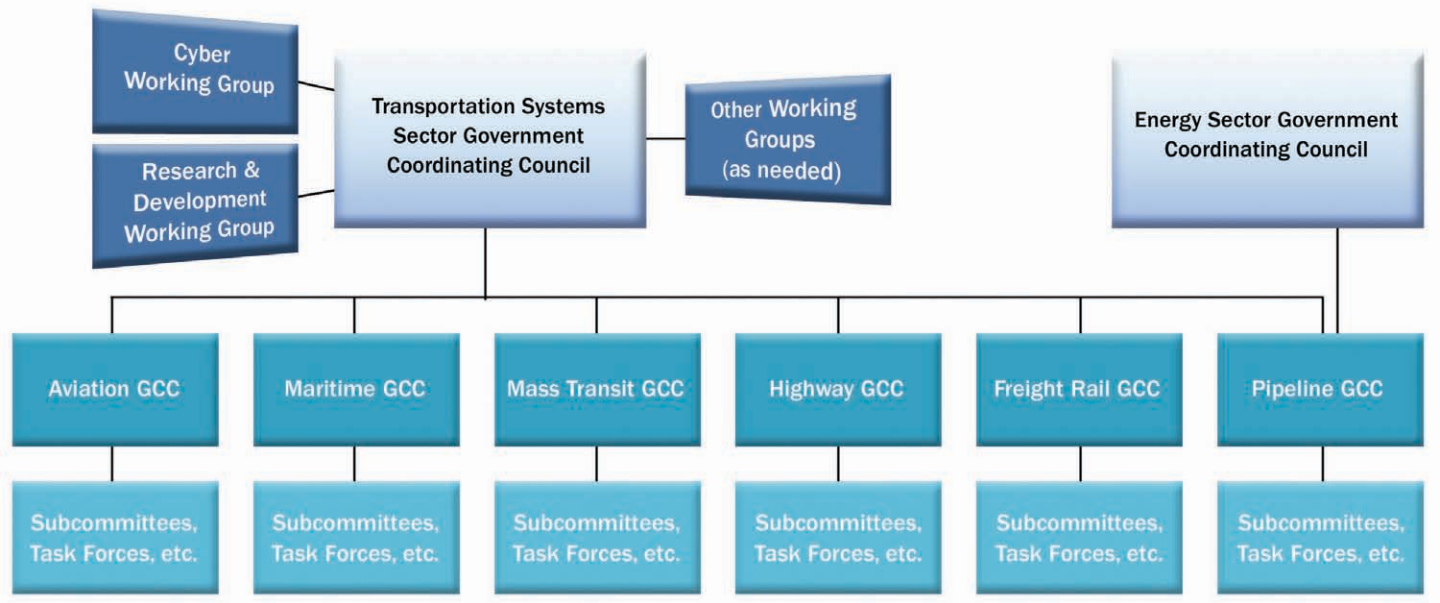


Figure 1-1 depicts the GCC organizational framework, including the relationship between the sector and modal level GCCs. The primary missions of the GCCs are to coordinate the development of transportation infrastructure protection and resiliency strategies and activities, to assure collaboration with 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.

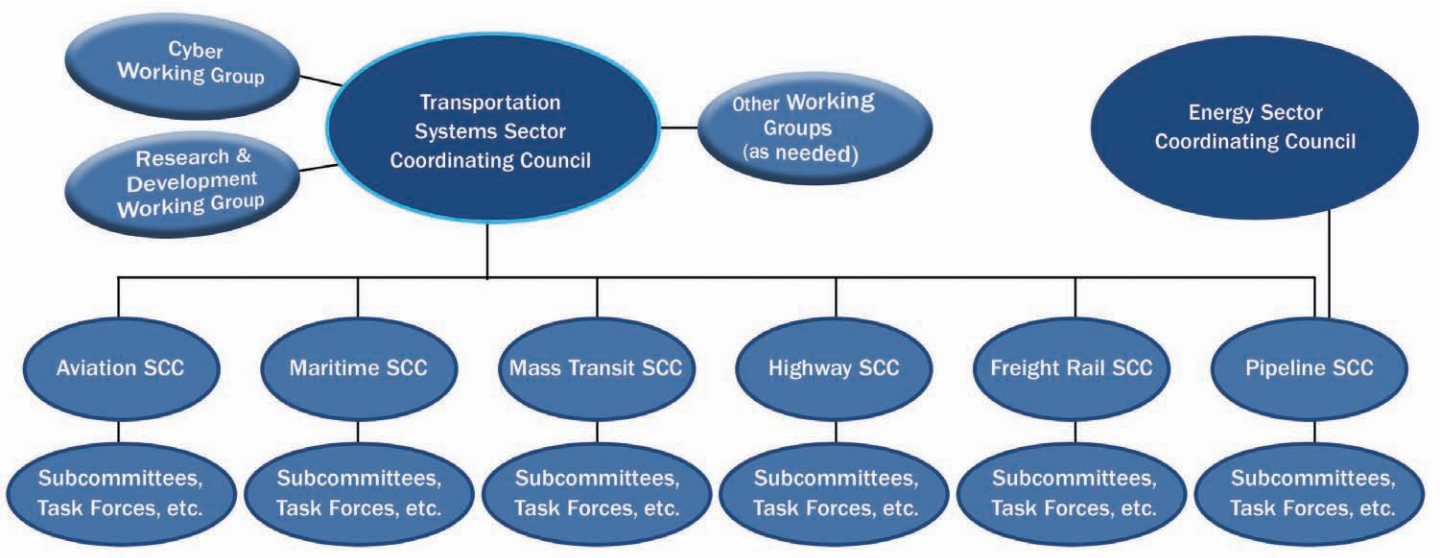
- Department of Commerce (DOC)
- Department of Energy (DOE)
- Department of Defense
- State, local, tribal, and territorial representatives

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

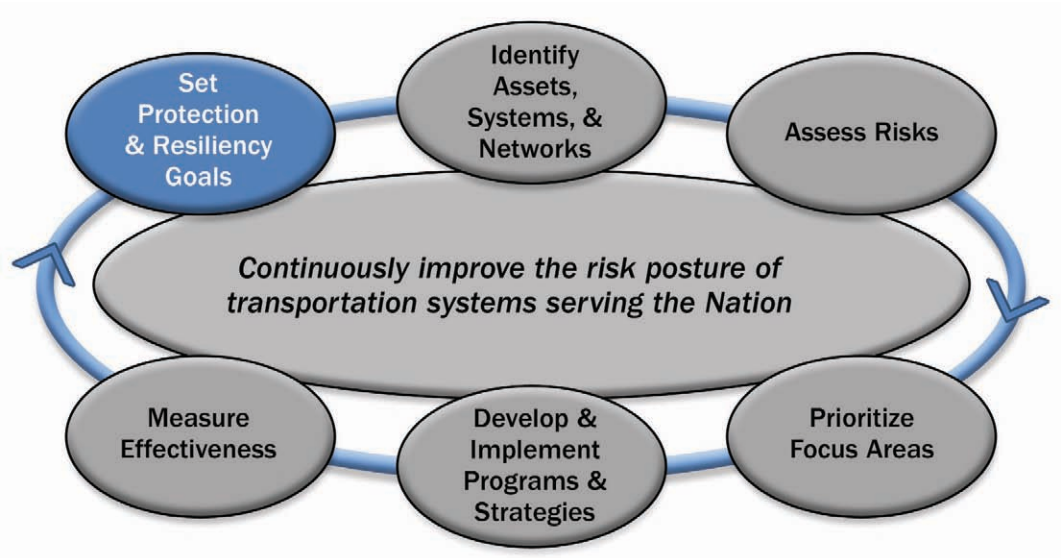
The sector's goals and objectives provided below are consistent with the goals outlined in the President's homeland security agenda, sector priorities, and the statutory imperatives for protecting the transportation system and improving resiliency of its critical infrastructure and networks. The President's 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.

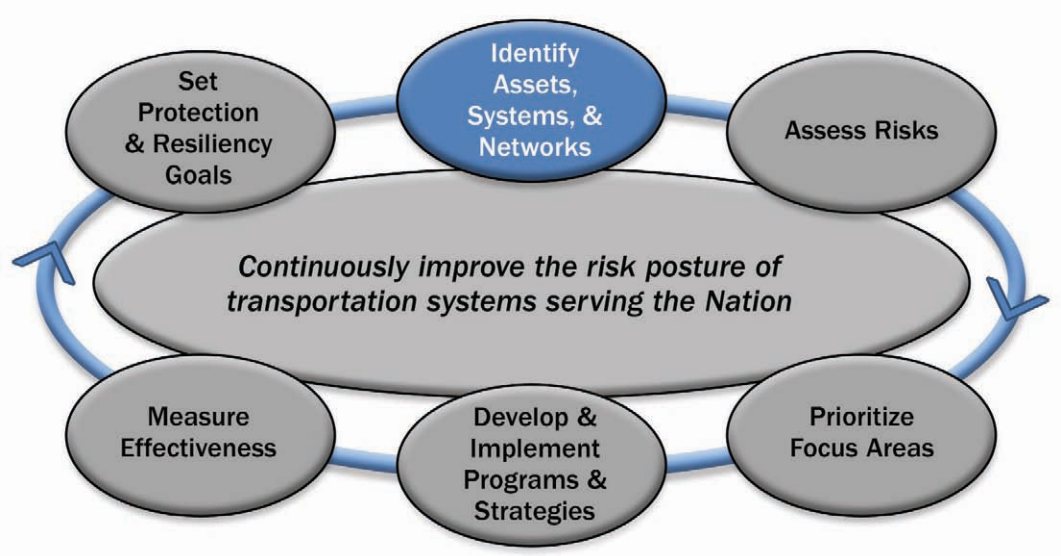
Objectives

- 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, subgroups, 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.

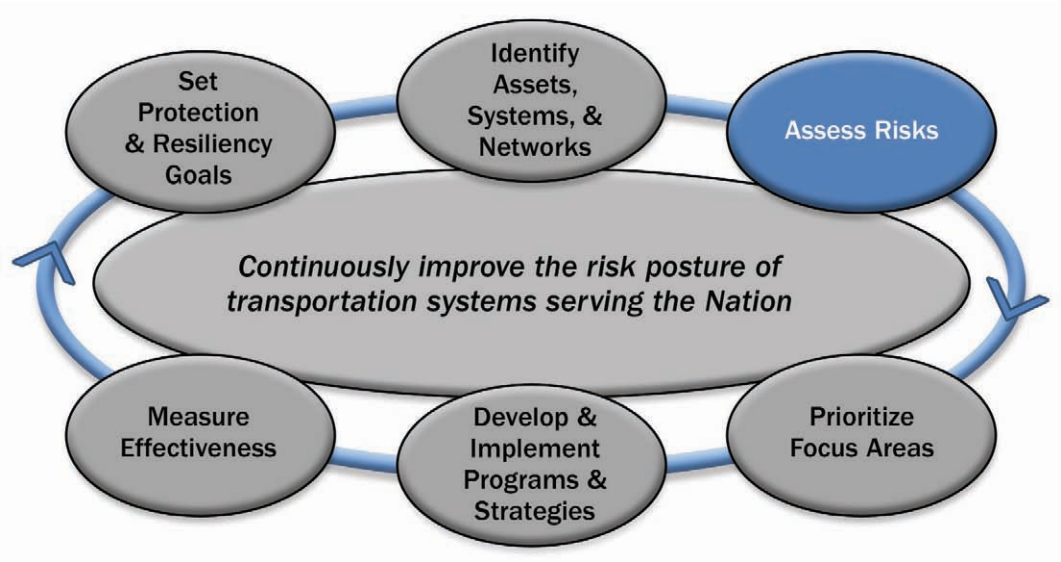
2.4 Critical Cyber Infrastructure Identification

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:

Risk = *f* (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:

Risk = *f* (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.

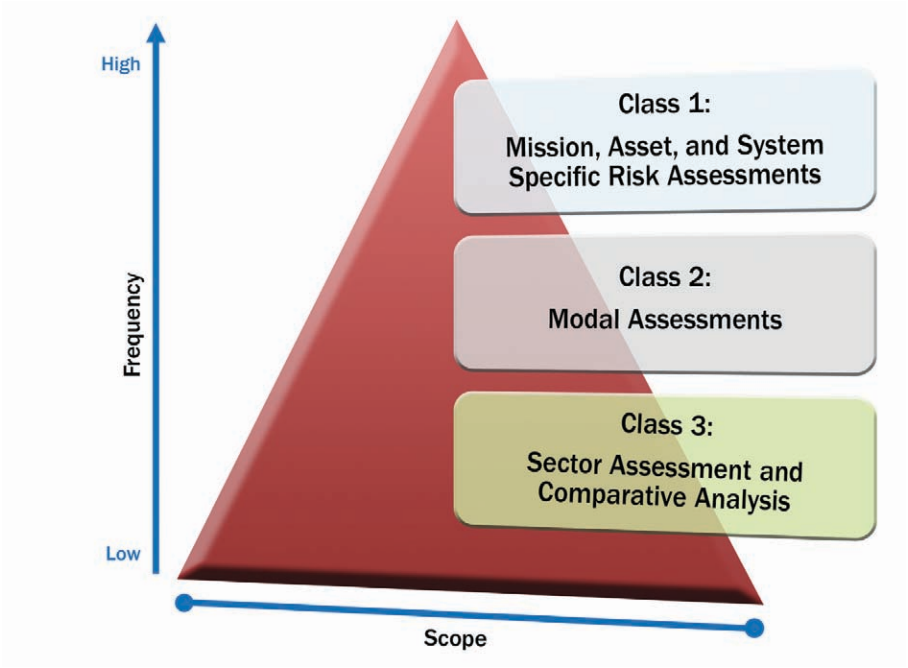
Assessments of transportation assets and systems consider information such as cargo or passenger volume, proximity to population centers, and system dependence on a particular asset. In refining the identification of transportation infrastructure assets, more detailed assessments may be useful to change 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 vulnerability[9] 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

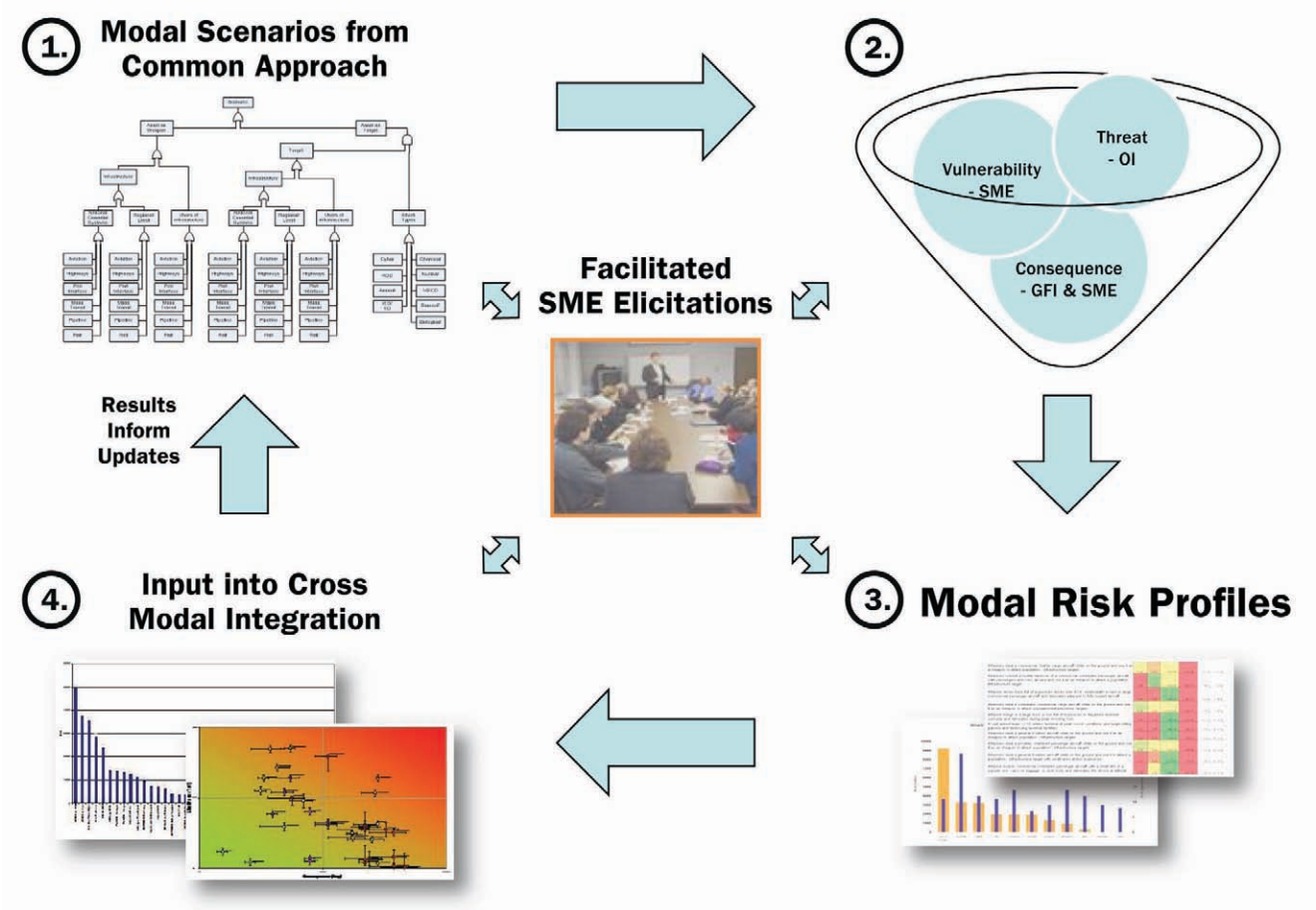
The following are brief descriptions of the primary risk assessment methods used by the six transportation modes along the three class levels. These tools and techniques are not directly mandated by or for specific modes, although some have been developed to fulfill legislative requirements.

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.

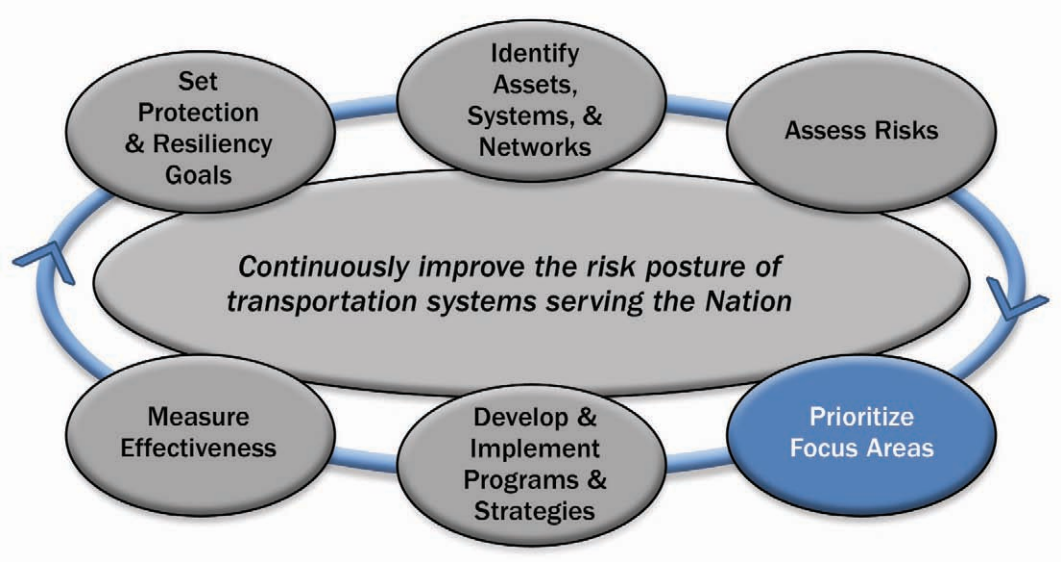
Assessment results should be quantifiable for use in subsequent risk analyses and metrics development.

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

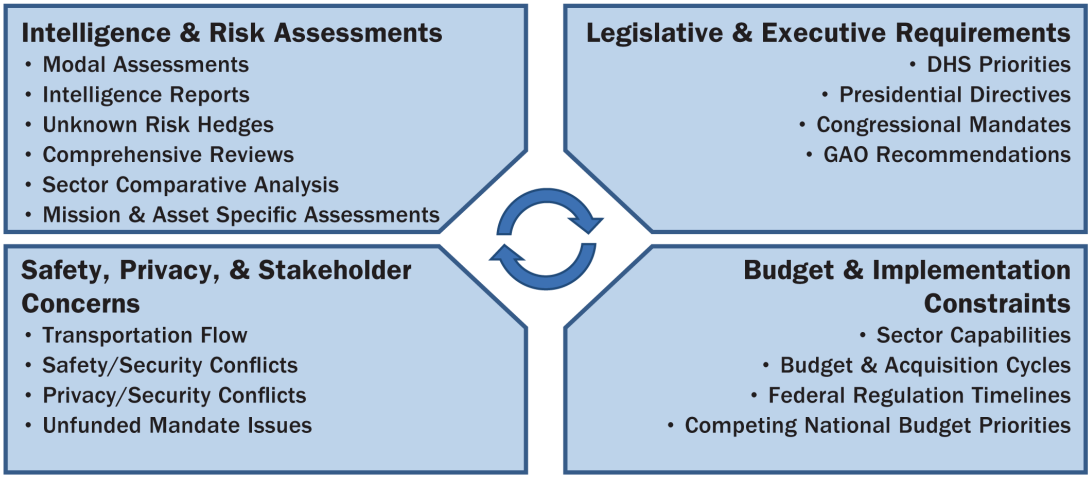


Chapter 3 described how risk assessments based on TVC data are used by the sector to inform resource allocation, as well as strategic and tactical planning. However, while risk assessments provide significant input to resource allocation decisions, other factors must also be considered. Various analytical 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

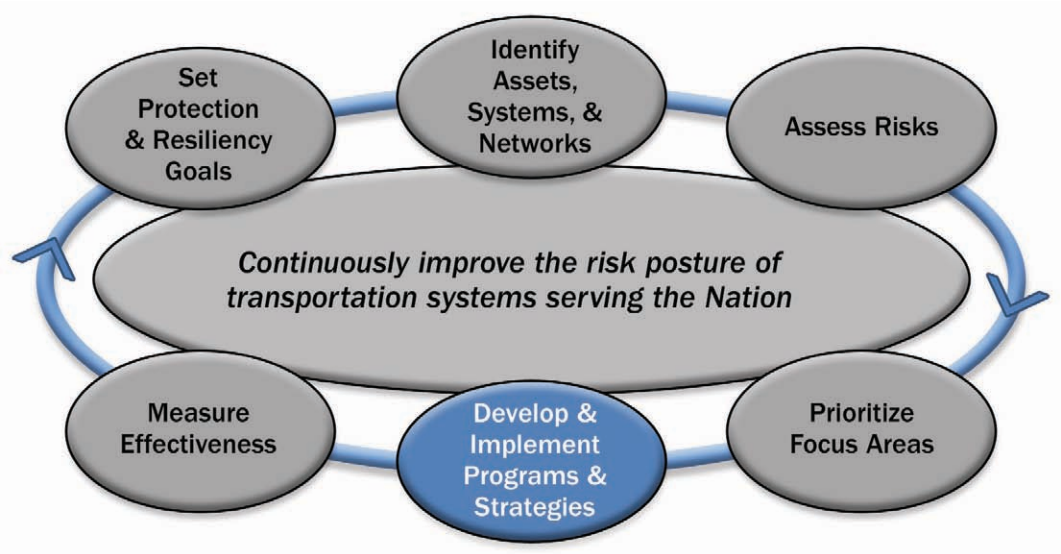
funds to implement legislated priorities. Consequently, the process for determining sector priorities considers fiscal elements in the decision environment for short-term and long-term impacts, in addition to the implications of risk assessments.

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.

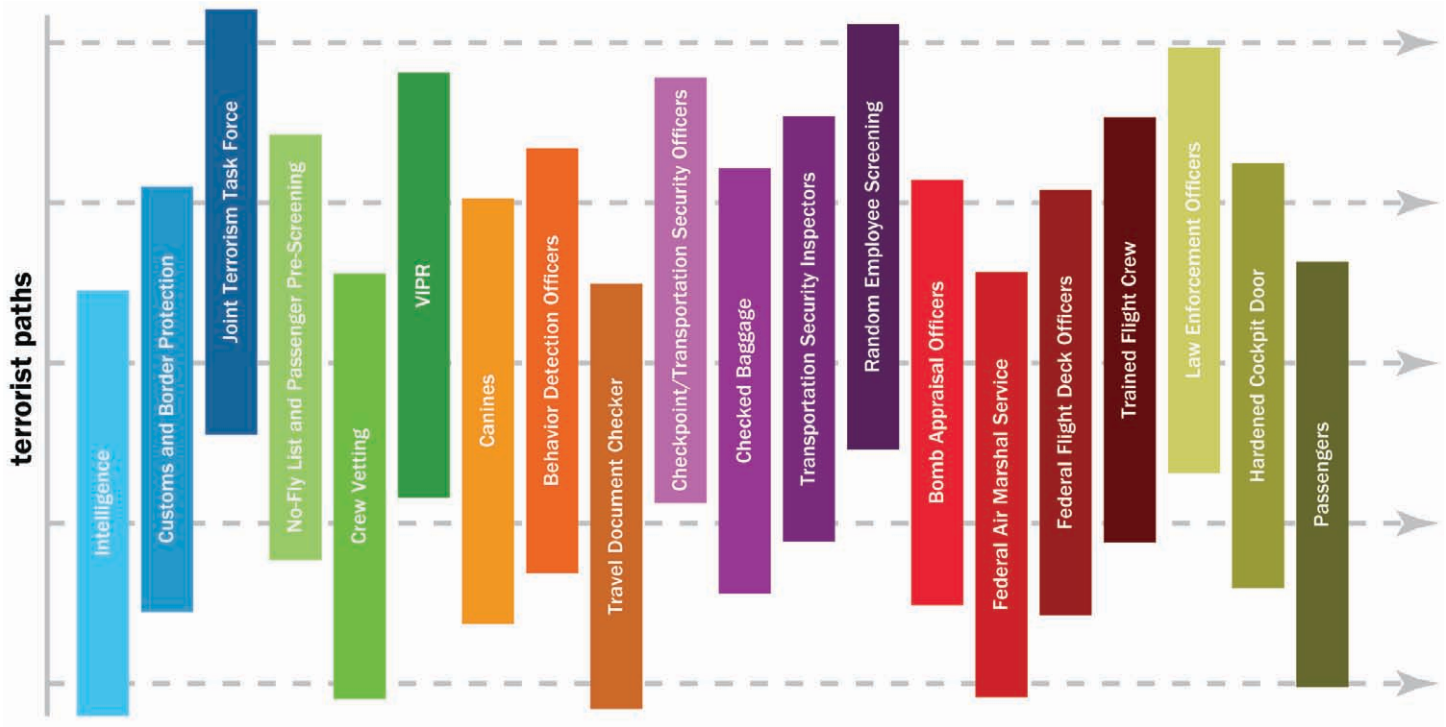
Federal, State, local, tribal, and territorial authorities, as well as the security personnel of owners and operators, provide this multi-jurisdictional layering before, during, and following an incident. A training vulnerability might be addressed through a set of layered training initiatives including 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 5-1.

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 5-1: 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.

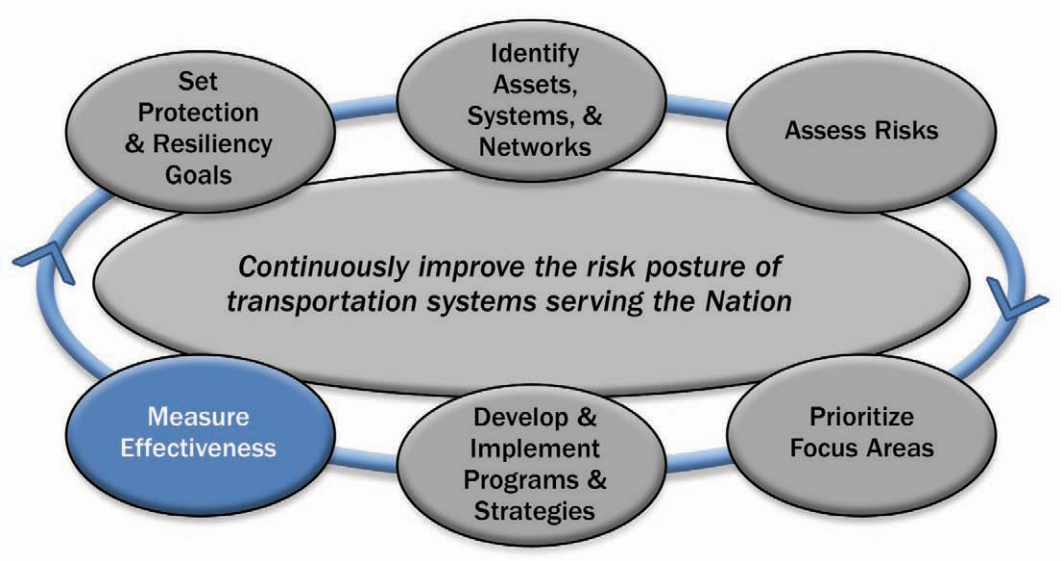
5.5 Monitoring Program Implementation

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 objectives[11] 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.	Develop technical standards and establish certified laboratories to evaluate homeland security and emergency responder technologies, and evaluate technologies for SAFETY Act protections. Develop ongoing cross-pollination activities (testing, studies, pilots, etc.) between government and stakeholder partners to expand the pool of available technologies to enhance security.
Improve sector situational awareness, understanding, and collaboration.	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. Develop layered, adaptive, secure nationwide enterprise architectures to facilitate shared situational awareness to enable real-time alerts to threats at an operational level. 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.

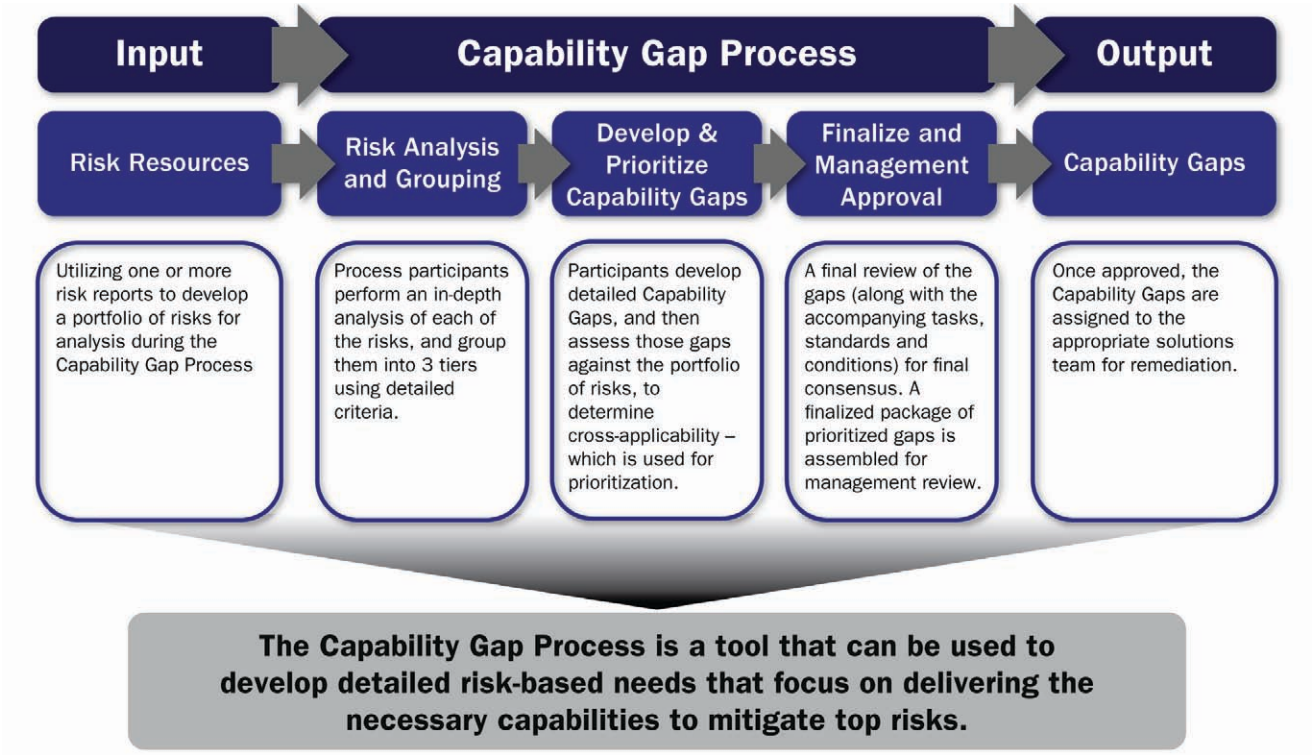
7.2 Sector R&D Needs

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.

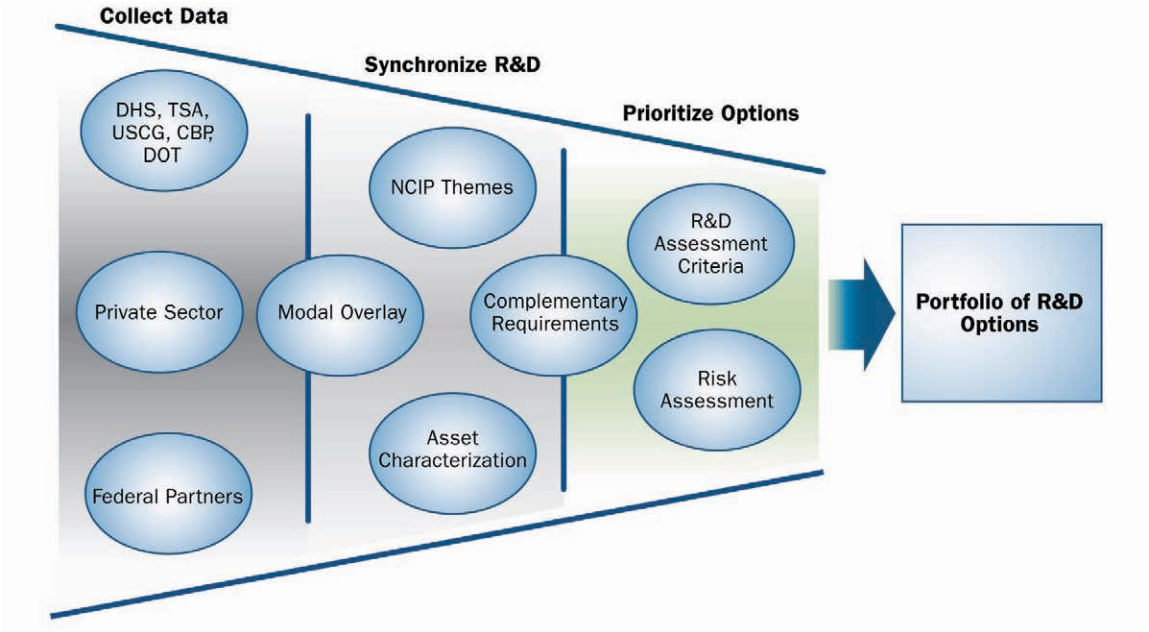
7.3 Sector R&D Plan

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:

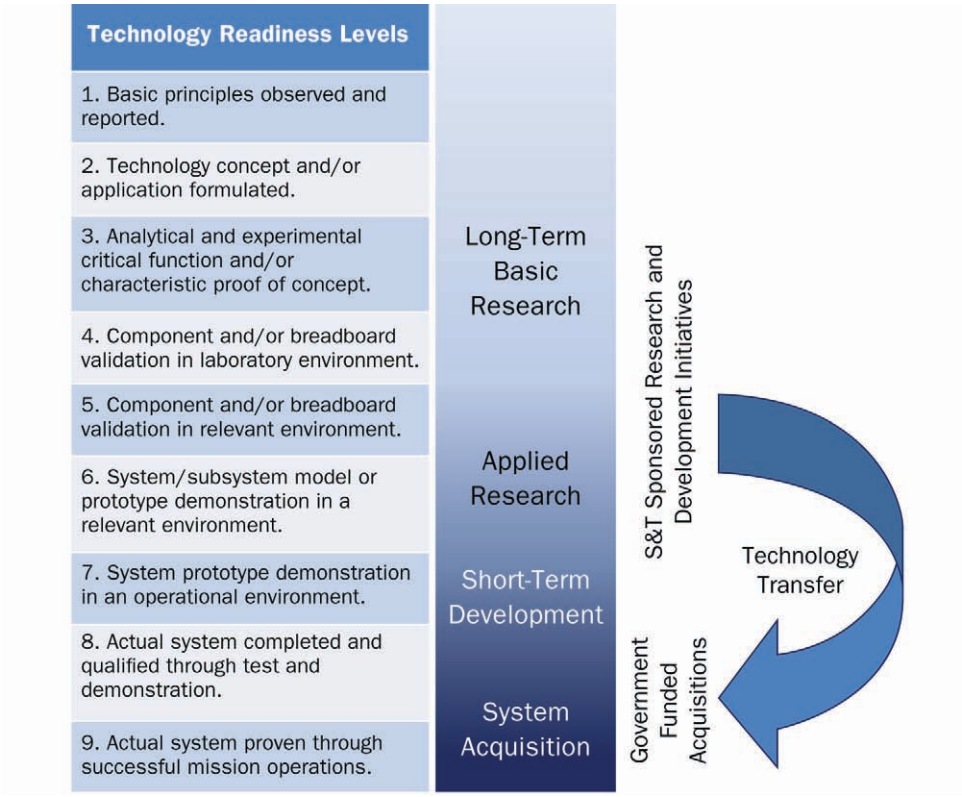
- Basic Research—The sector looks to the national laboratories and academia to complete long-term basic research. S&T utilizes the expertise of nine national laboratories under Section 309 of the HSA of 2002. Academia has been directly engaged through a number of activities, ranging from the funding 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



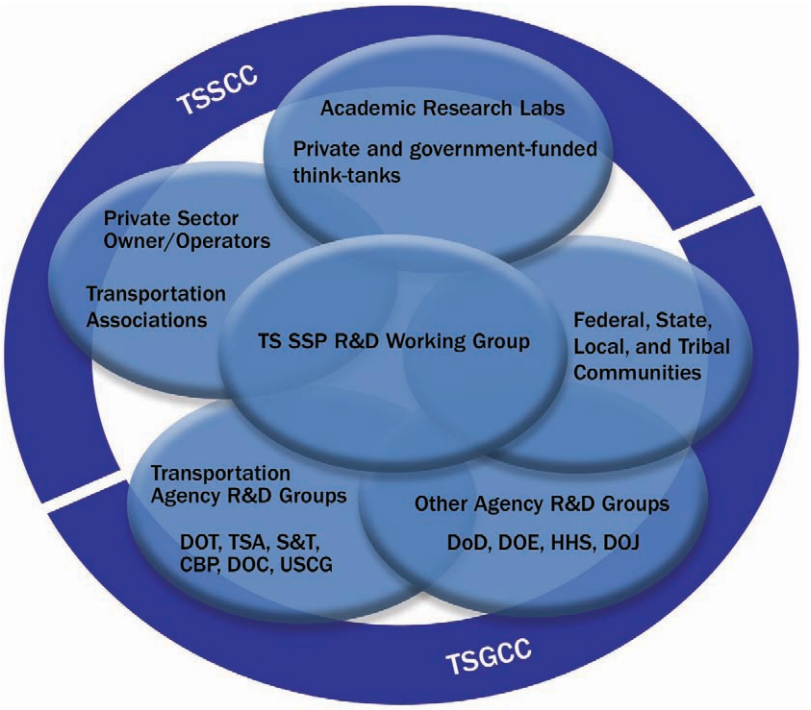
7.4 Sector R&D Management Process

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.

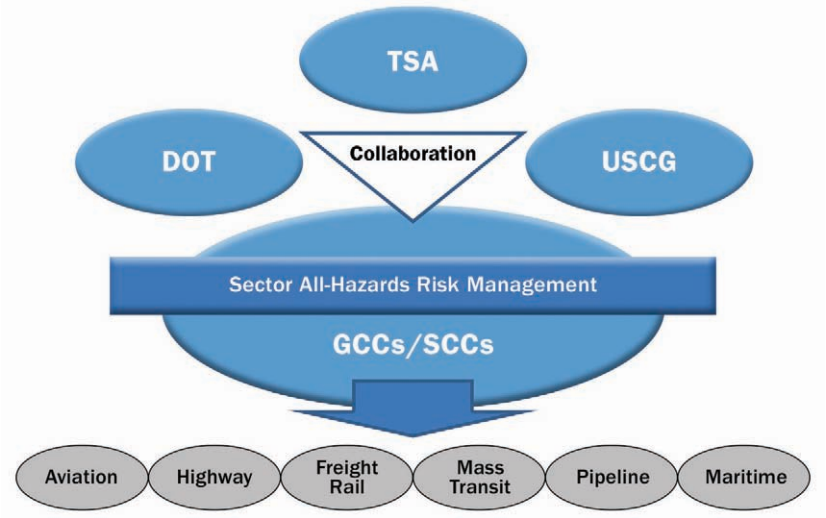
8. Managing and Coordinating SSA Responsibilities

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.

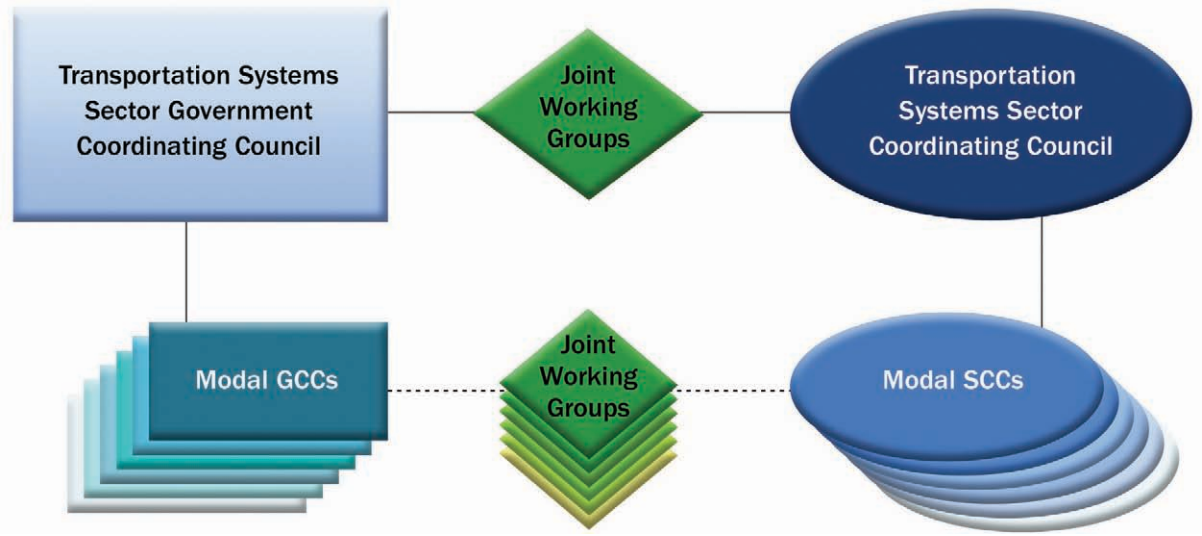
Figure 8-1: Transportation Systems Sector Management Approach



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	• Conduct annual review and validation/update based on process feedback • Update modal cybersecurity objectives for modal specific and intermodal concerns
	• 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	• Participate in annual DHS NCIPP and the Critical Foreign Dependencies Initiative
	• 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	• Refine the sector strategic risk assessment model for the annual risk assessment requirement
	• 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	• Update priorities based on annual assessments
	• 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	• 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
	• 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	• Work with government partners and DHS IP to meet the NIPP's annual metrics milestones
	• 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 incorpo-

[14] **https://www.dot.gov/disaster_recovery/resources/DOT_NTRS.pdf**.

rates 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.

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)

[15] **http://www.fas.org/irp/agency/ise/plan1106.pdf**.

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 interagency 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 coop¬eration, 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 leader¬ship 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).** PMHSA 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 transportations 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

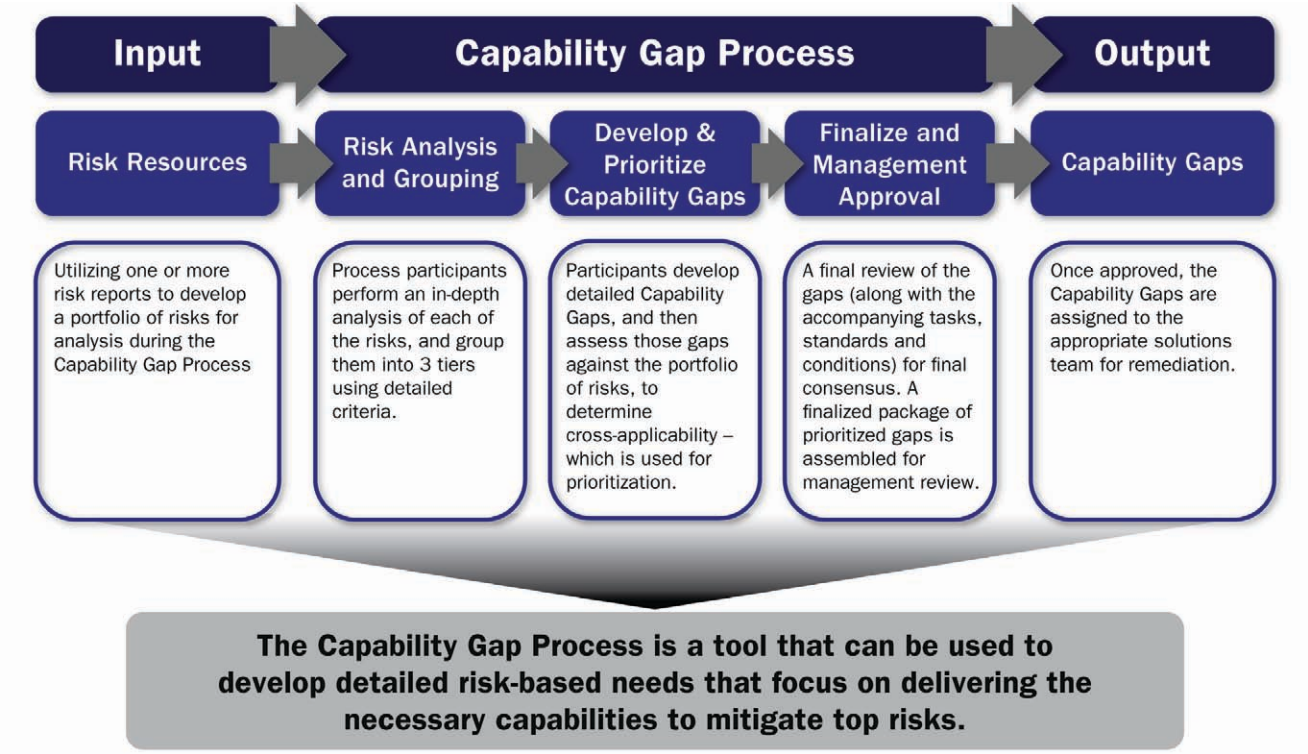
of DOT, DoD, DHS, DOS, and other sector partners. These activities are accomplished through the examination, evaluation, and testing of innovative technologies, policies, procedures, organizational improvements, or a combination of these, and by the design, rapid prototyping, and deployment of integrated 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 FHA 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

* 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.

** 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.

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: ➢ 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: ➢ 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.

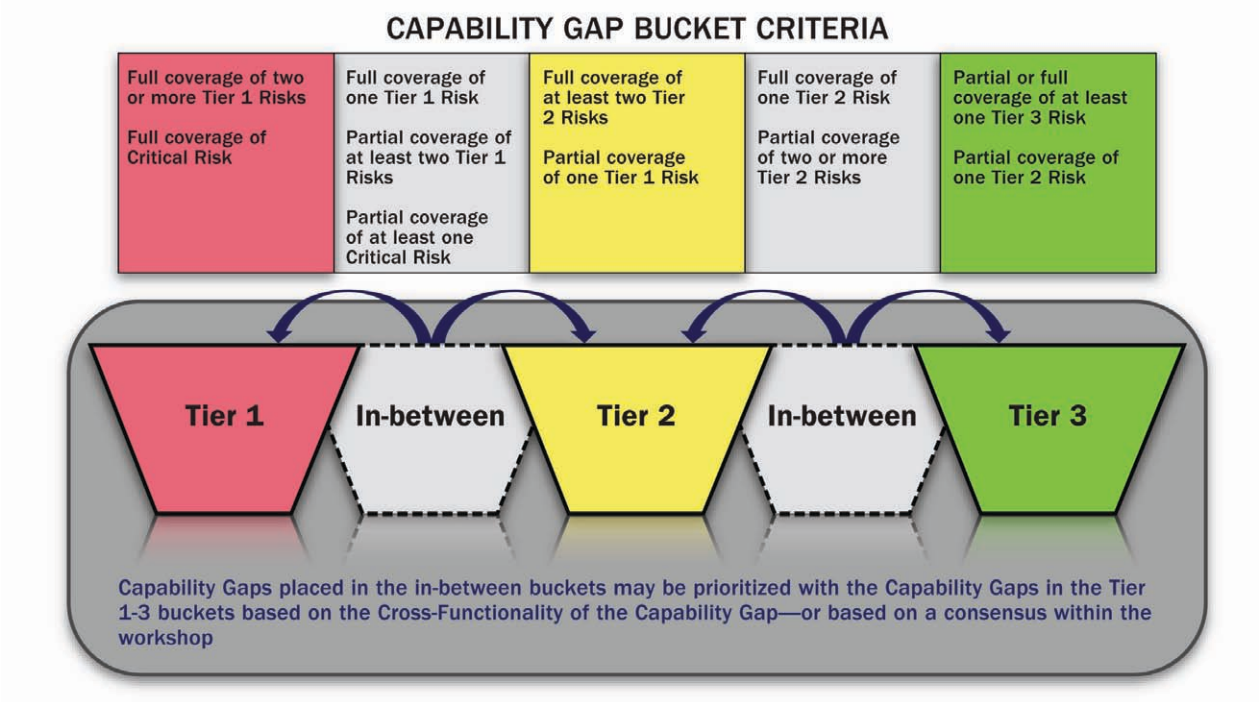
Once the gaps are revised, they are assessed across the previously identified risk groups. The prioritization process is based on criteria that take into account both the grouping of the risks they address as well as the number of risks they cover. Thus, higher importance is placed on capability gaps 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. *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.*
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.) *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.*
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.) *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.*

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 be 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**	
	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 of products through the defined systems. The individual assets provided in this taxonomy, then, are the physical elements that comprise the systems of interest.	
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. *Barges designed to carry gaseous materials.*
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 interstate 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

List of Figures

List of Tables

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 interagency 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

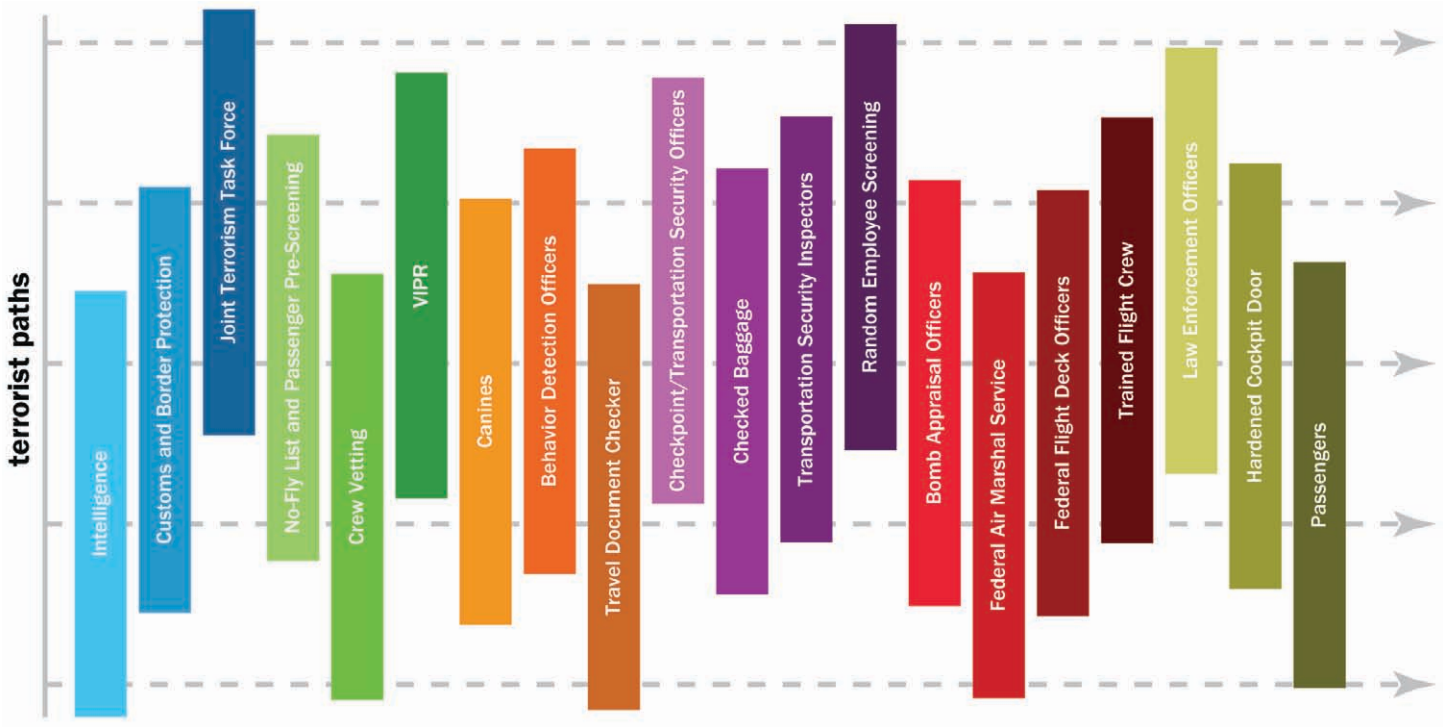
TSA has also partnered with industry to create the Risk Management Analysis Process (RMAP), an innovative risk evaluation method that uses an agent-based, Monte Carlo simulation model to provide insights for security countermeasure investment decisions. RMAP supports the aviation mode by using subject 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 representativies 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 • 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

List of Figures

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 Responsibilities[3]

C: Plan to Re-establish Cargo Flow After a Transportation Security Incident[4]

D: Maritime Security (MARSEC) Levels[5]

E: Maritime Enterprise Mapping: Directives and Guidance[6]

[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 domain[7] are the primary mode of transportation for world trade, carrying more than 80 percent[8] 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 Recommendations[13] 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 sources[20] 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 as 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 port[24] 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 (DWPs) 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 Report[27] 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 Consultation[37] 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.

Homeport[41]

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 is 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**.

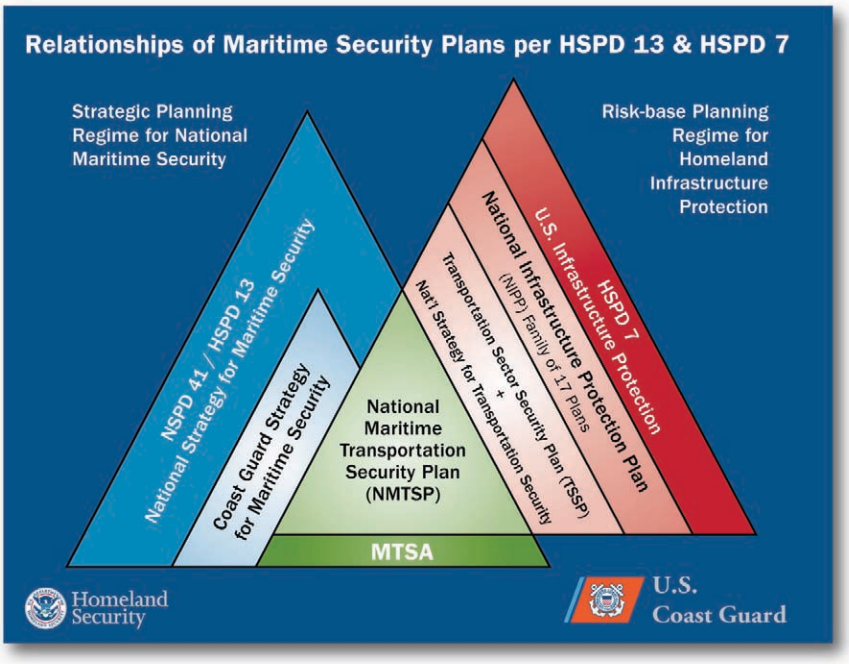
3. The Implementation Plan

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.

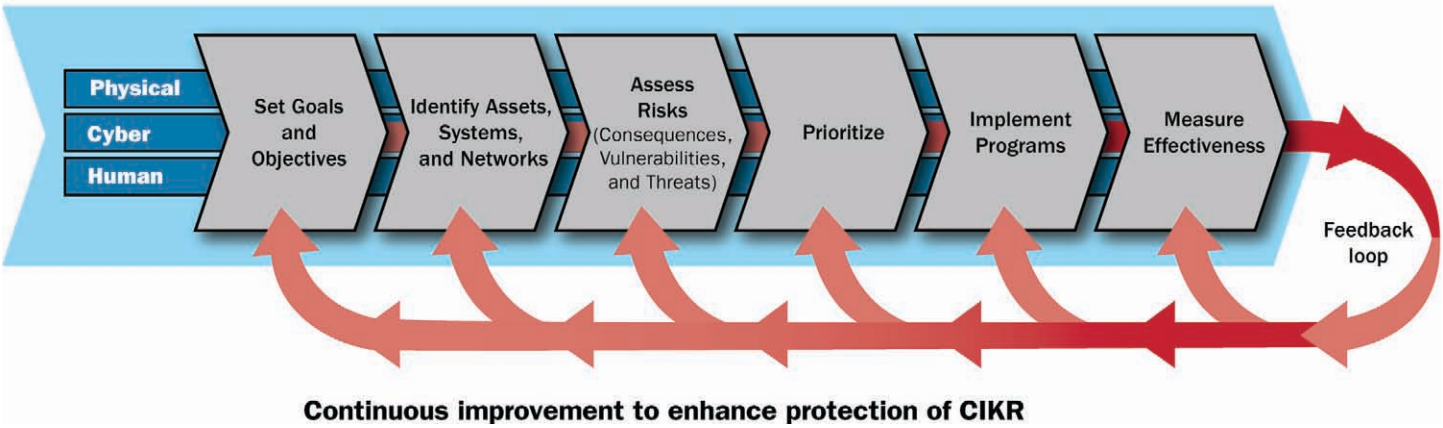
The SSA participates in the annual prioritization of Level 1 and Level 2 assets, and in the Critical Foreign Dependencies Initiative through the National Critical Infrastructure Prioritization Program, which fulfills the requirements of the Implementing Recommendations of the 9/11 Commission Act to produce 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 Risk = f (Threat x Vulnerability x 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 multimission 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 Regime[48]

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

List of Figures

List of Tables

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 2007[1] 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 programs[17] 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, 9/11Act.

[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 plan[22] 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.

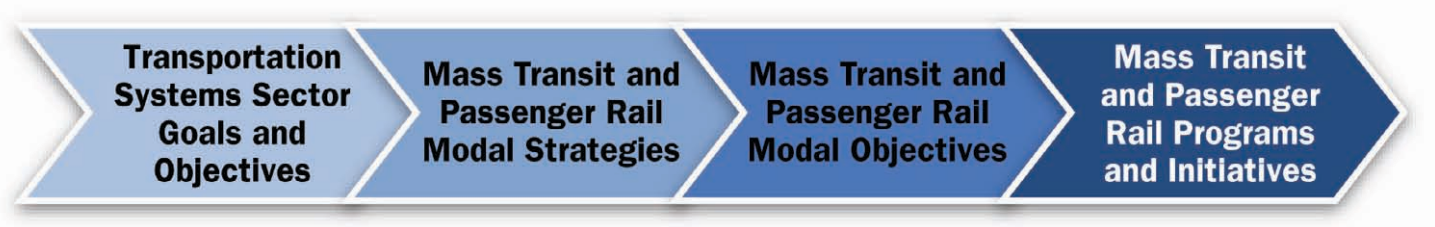
3. Implementation Plan

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 -
• Employ technology for screening passengers and bags in random applications throughout the mass transit and passenger rail systems as appropriate.
• Bolster screening technology efforts with a program for random searches of passengers' bags entering system.
• 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.
• Focus resources and efforts towards hardening the Nation's most critical mass transit and passenger rail assets.
• 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 gleaning 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 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

List of Figures

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.

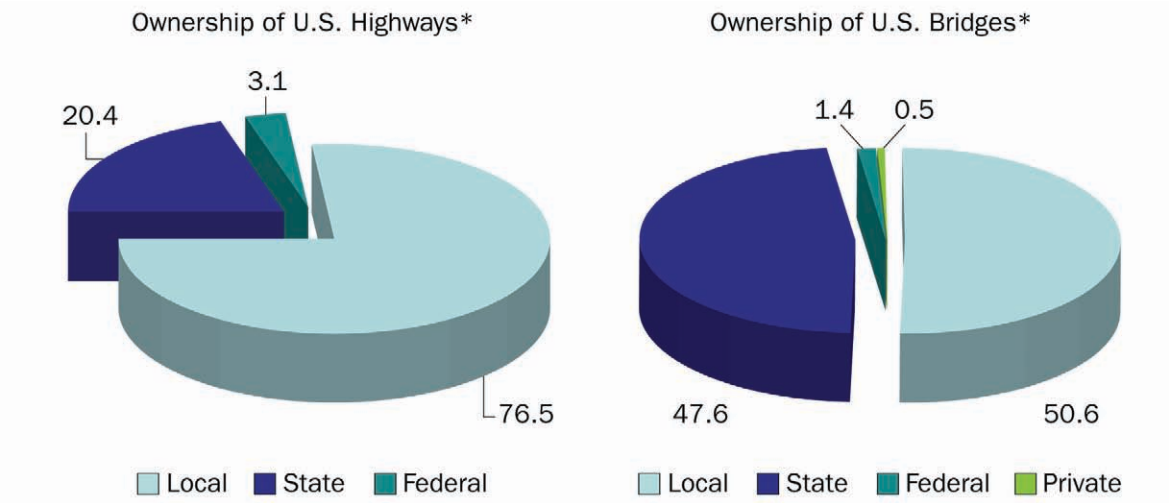
Toward this end, DHS, DOT, and private sector security partners continue to be committed to improving the highway transportation system. Technology and security awareness and expertise must keep pace with the increasingly sophisticated terrorist or criminal techniques that may be used to threaten the 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.

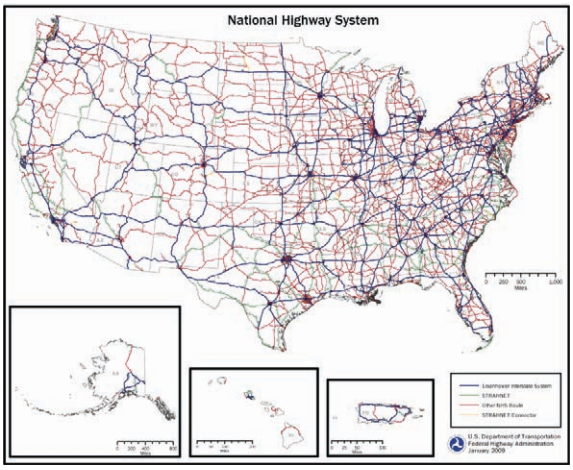
protection of its critical infrastructure. State and local governments and businesses, however, are essential partners with the Federal government in the development and operation of the Nation's highway network.

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:

Risk = *f* (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 Requirements[6]

- 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 website[7] 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 devises (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-232[8] 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

List of Figures

List of Tables

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 materials[1] (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 railroads[5] 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 shipments[10] 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 Macdona, 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, Macdona, 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.

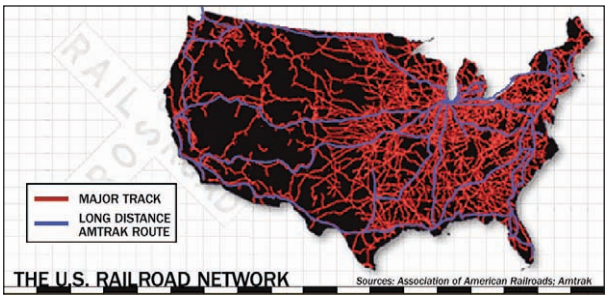
TSA and industry security partners use threat analysis to complete comprehensive risk assessments and risk mitigation activities. The risk management framework strikes a balance between developing ways to mitigate both specific and general threats. The framework permits the range of plausible attack 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.

Risk = *f* (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:

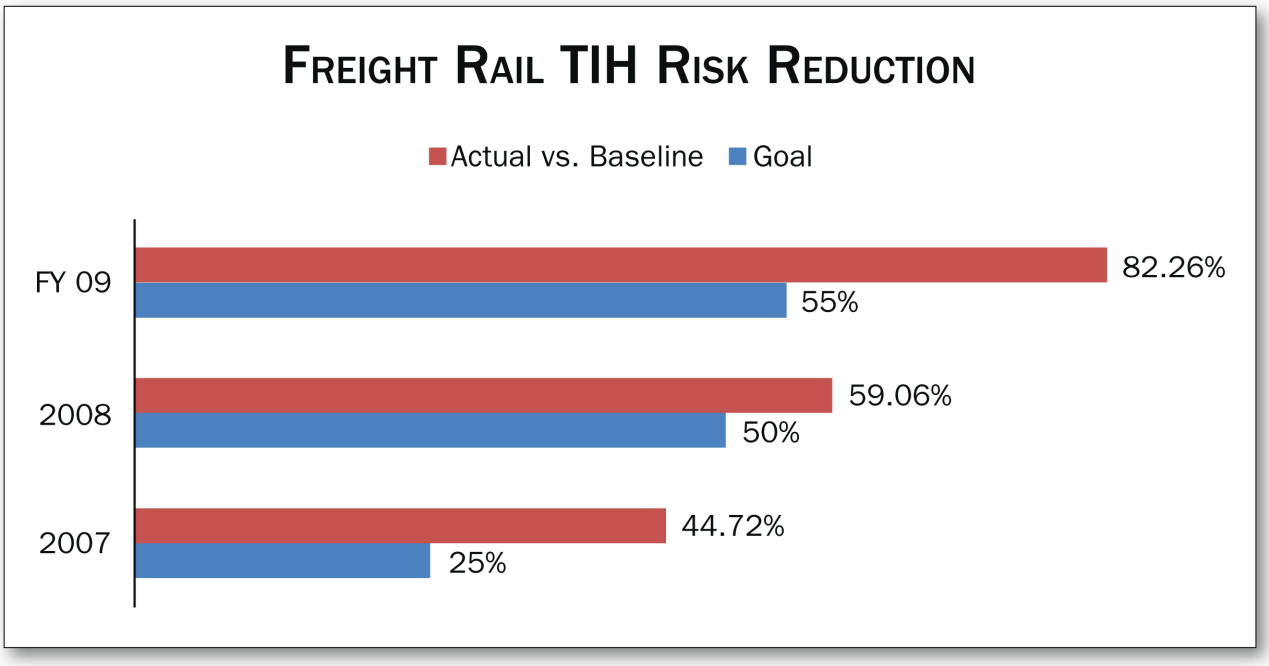
- **Total hours TIH cars were present inside an HTUA.** TSA collects data from the rail industry's automated systems that record the movement and location of all rail cars within the U.S. rail system by means of electronic identification tags. TSA uses these data to quantify the amount of time TIH rail 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 indictor, 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 provisions[18] 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 items[19] 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.

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 FRSGP 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		
	Primary Gaps and Initiatives	Reduce the Vulnerability of Cargo	Reduce the Vulnerability of the Network	Reduce the Consequences of Attack
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

List of Figures

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

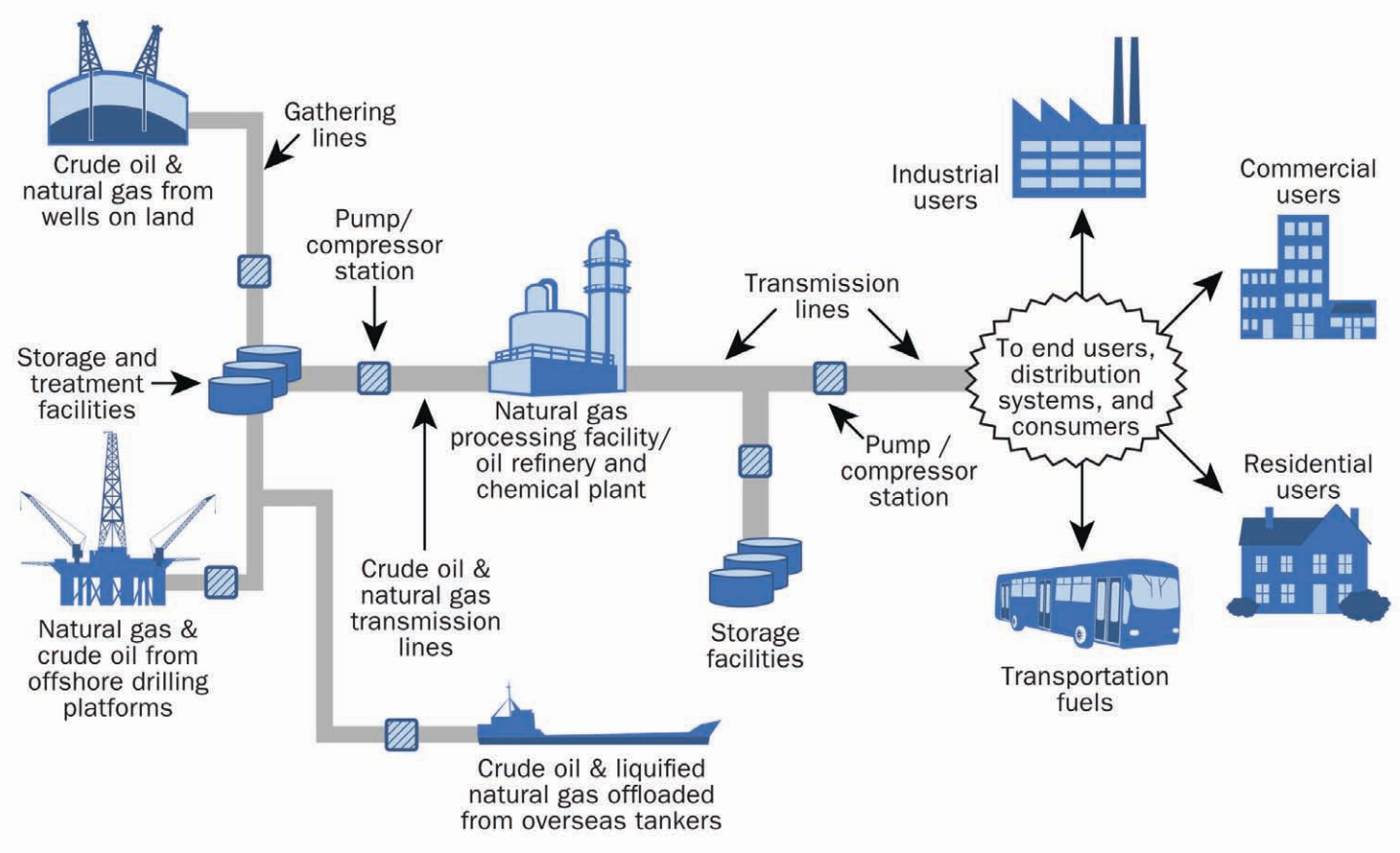
The following are the main types of pipelines:[2]

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.

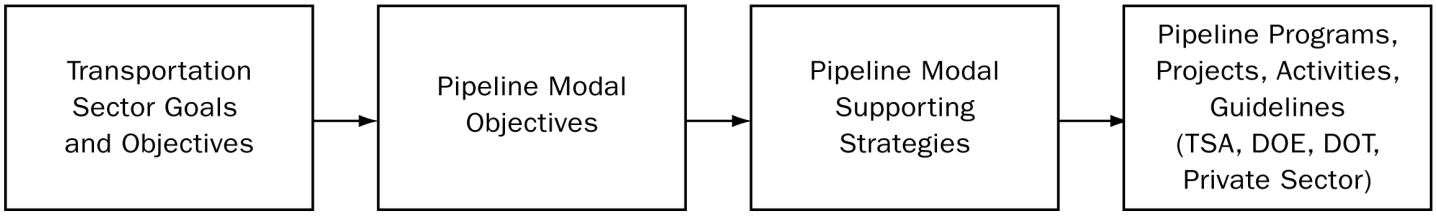
3. Implementation Plan

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

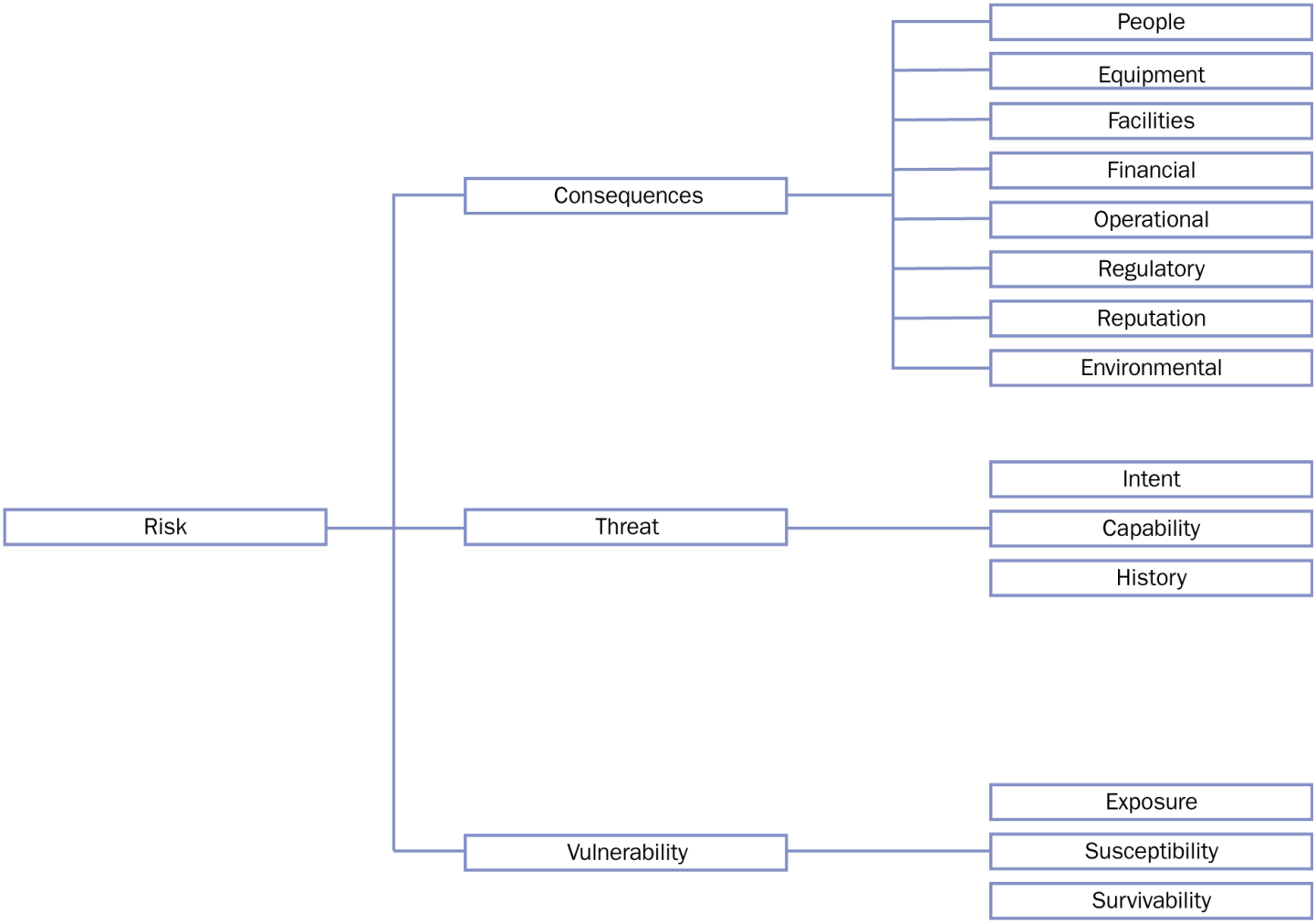
This section explains the pipeline risk assessment method that the TSA Pipeline Security Division utilizes.

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

3.5.2 Other Federal Agency-Led Programs, Projects, and Activities -

Program/Project/ Activity	Description	Participants	Pipeline Strategies Supported
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/ Sponsor-ship 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.shtm**.

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	• 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	• 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	• 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	• 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	• 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	• DOT-sponsored Contingency, Resiliency, Response, Restore Training/Workshops • TSA Pipeline Security Awareness Training CD • API/AGA Workshops	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	• 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	• Relative Risk Ranking Tool	

Homeland Security