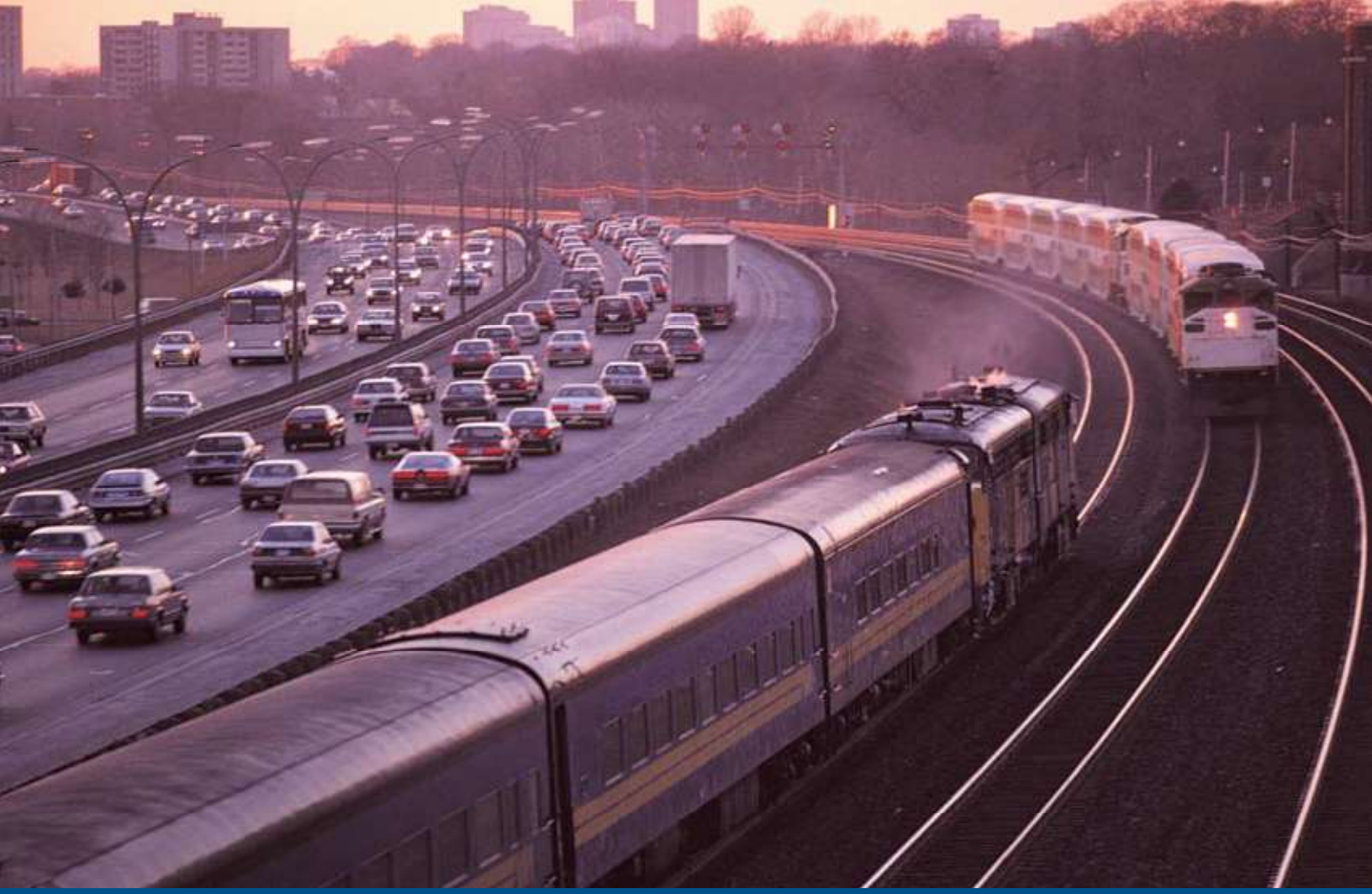


Transportation Systems

Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan

May 2007

Homeland Security

U.S. Department of Homeland Security
Arlington, VA 22202

Transportation Security Administration

The National Infrastructure Protection Plan (NIPP) provides the unifying structure for the integration of Critical Infrastructure and Key Resources (CI/KR) protection efforts into a single national program. The NIPP provides an overall framework for integrating programs and activities that are underway in the various sectors, as well as new and developing CI/KR protection efforts. The NIPP includes 17 sector-specific plans (SSPs) that detail the application of the overall risk management framework to each specific sector.

Each SSP describes a collaborative effort between the private sector; State, local and tribal governments; nongovernmental organizations; and the Federal Government. This collaboration will result in the prioritization of protection initiatives and investments within and across sectors to ensure that resources can be applied where they contribute the most to risk mitigation by lowering vulnerabilities, deterring threats, and minimizing the consequences of attacks and other incidents. By signing this letter, the members of the Transportation Sector Government Coordinating Council (TSGCC) commit to:

- Support the Transportation SSP concepts and processes, and carry out their assigned functional responsibilities regarding the protection of CI/KR as described herein;

- Work with the Secretary of Homeland Security and the Assistant Secretary of Homeland Security for Transportation Security, as appropriate and consistent with their own agency-specific authorities, resources, and programs, and to coordinate funding and implementation of programs that enhance CI/KR protection;

- Cooperate and coordinate with the Secretary of Homeland Security and the Assistant Secretary of Homeland Security for Transportation Security, in accordance with guidance provided in Homeland Security Presidential Directive 7, as appropriate and consistent with their own agency-specific authorities, resources, and programs, to facilitate CI/KR protection;

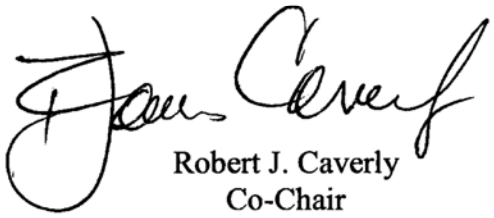
- Develop or modify existing interagency and agency-specific CI/KR plans, as appropriate, to facilitate compliance with the Transportation SSP;

- Develop and maintain partnerships to CI/KR protection with appropriate State, regional, local, tribal, and international entities; the private sector; and nongovernmental organizations; and

- Protect critical infrastructure information according to the Protected Critical Infrastructure Information Program or other appropriate guidelines, and share CI/KR protection-related information, as appropriate and consistent with their own agency-specific authorities and the process described herein.

At present, the Transportation Sector Coordinating Council (TSCC) is in the process of being formed, but the process is not complete. The TSGCC enthusiastically endorses the formation of the TSCC and we look forward to advancing the Transportation Sector Specific Plan together with these key stakeholders.

John P. Sammon
Co-Chair
Transportation Sector Government Coordinating Council
Transportation Security Administration
Department of Homeland Security



Robert J. Caverly
Co-Chair
Transportation Sector Government Coordinating Council
Office of Infrastructure Protection
Department of Homeland Security

Table of Contents

List of Figures

List of Tables

Executive Summary

Transportation Security Environment

The Transportation Systems Sector-Specific Plan—a sector that comprises all modes of transportation (Aviation, Maritime, Mass Transit, Highway, Freight Rail, and Pipeline)—is a vast, open, interdependent networked system that moves millions of passengers and millions of tons of goods. The transportation network is critical to the Nation's way of life and economic vitality. Ensuring its security is the mission charged to all sector partners, including government (Federal, State, regional, local, and tribal) and private industry stakeholders. Every day, the transportation network connects cities, manufacturers, and retailers, moving large volumes of goods and individuals through a complex network of approximately 4 million miles of roads and highways, more than 100,000 miles of rail, 600,000 bridges, more than 300 tunnels and numerous sea ports, 2 million miles of pipeline, 500,000 train stations, and 500 public-use airports.

The sector's security risks are evident by attacks either using or against the global transportation network, including not only the September 11, 2001, attacks on the World Trade Center and the Pentagon, but also more recent attacks on transportation targets such as the 2005 London bombings, the coordinated attack on four commuter trains in Madrid in 2004, and the 2006 plot uncovered in the United Kingdom targeting airlines bound for the United States. These recent attacks are a sobering reminder that the transportation system remains an attractive target for terrorists post-September 11. Hurricane Katrina and other disasters (natural and industrial) also highlight the risk to the sector that is not directly related to terrorism. Taken together, the risk from terrorism and other hazards demands a coordinated approach involving all sector stakeholders.

In the wake of the September 11 attacks, the Transportation Systems Sector-Specific Plan joined together in an unprecedented way to protect its customers, systems, and assets. The private sector has made great contributions in sector-wide risk-reduction efforts, often of their own volition. State and local governments likewise reacted swiftly to the attacks, enhancing first-response capabilities, increasing vigilance, and securing potential targets. This type of cooperation among the diverse sector stakeholders is one of the strengths of the Transportation Systems Sector-Specific Plan.

In addition to ongoing efforts, there is a distinct set of strategic risks where the Federal Government will add special value. These risks exhibit two distinguishing characteristics: First, they present issues that raise complex implementation issues for industry, and State and local governments. Second, they have a very high materiality (i.e., very significant consequence and plausible likelihood). Strategic risks, such as the use of some element of the transportation network as a weapon of mass destruction (WMD), have a multi-jurisdictional and sector-wide effect. Therefore, Federal involvement will improve the sector's risk management posture by focusing on system-wide risk.

In the face of the reality that terrorists will continue to target the transportation network, a systems-based risk management (SBRM) strategy that lays out a strategic framework to improve the sector's risk management posture is necessary. This strategy focuses on implementing multiple layers of security to defeat and deter the more plausible and dangerous forms of

attack against the Nation's transportation network. Importantly, the SBRM process is strategic in nature, yielding strategic countermeasures, and does not directly address operational or tactical plans. The National Infrastructure Protection Plan (NIPP), signed by Michael Chertoff, Secretary of the Department of Homeland Security (DHS), in June 2006, as a requirement of Homeland Security Presidential Directive 7 (HSPD-7), obligates each critical infrastructure and key resources (CI/KR) sector to develop a Sector-Specific Plan (SSP) that describes strategies that protect the Nation's CI/KR under their purview, outline a coordinated approach to strengthen their security efforts, and determine the appropriate programmatic funding levels.

The Transportation Systems SSP and its supporting modal implementation plans and appendices establish the Transportation Systems Sector-Specific Plan's strategic approach based on the tenets outlined in the NIPP and the principles of Executive Order 13416, Strengthening Surface Transportation Security. The Transportation Systems SSP describes the security framework that will enable sector stakeholders to make effective and appropriate risk-based security and resource allocation decisions.

To be effective, a strategic plan must define a vision and mission statement, coupled with targeted goals and objectives to which operational and tactical efforts are anchored. Section 1 of the Transportation Systems SSP provides a robust discussion of how the sector's security vision, mission, goals, and objectives were developed and agreed to by the sector's security partners through the Government Coordinating Council (GCC)/Sector Coordinating Council (SCC) framework.

Vision Statement for the Transportation Systems Sector

Our vision is a secure and resilient transportation network, enabling legitimate travelers and goods to move without undue fear of harm or significant disruption of commerce and civil liberties.

Mission Statement for the Transportation Systems Sector

Continuously improve the risk posture of the Nation's transportation system.

Goals:

1. Prevent and deter acts of terrorism using or against the transportation system;
2. Enhance the resilience of the transportation system; and
3. Improve the cost-effective use of resources for transportation security.

The vision and mission statement for the Transportation Systems Sector-Specific Plan establish a foundation upon which the sector's prioritization and resource allocation processes are built. The risk-informed, decisionmaking process, detailed in sections 3 through 5, outlines how strategic risk objectives (SRO) developed through the GCC/SCC framework will be formulated, continuously evaluated, and updated to reflect shifting priorities or changes in the security environment.

A Systems-Based Risk Management Approach to Transportation Security

The NIPP defines risk as a function of threat, vulnerability, and consequence. Analysis of risk and the evaluation of countermeasures require consideration of all three variables. The Transportation Systems Sector is a complex network with six interdependent modes. Disruptions in the transportation network can often have nonlinear effects. As a result, what may initially appear as an isolated disturbance in the network can have a much greater, sector-wide impact.

One of the critical challenges facing the Transportation Systems Sector is understanding the downstream implications of potential disruptions. For example, following the September 11 attacks, the aviation system was shut down and the borders were closed, causing supply chain disruptions across multiple industries. Recognizing the importance of systems is key when determining cost-effective countermeasures. Since resources available for protecting CI/KR are discretely limited, a robust decisionmaking process that provides critical information to identify the highest priority systems and assets is necessary. To meet this need, the Transportation Systems SSP outlines a structured, eight-step SBRM approach that augments the NIPP risk management framework and looks beyond protecting a single asset or set of assets. One major benefit of adopting and implementing the SBRM approach is that the sector will have a process that includes Federal, State, regional, local, and private sector experience and creativity to leverage limited resources and develop countermeasures.

Introducing SBRM does not represent a sudden change of course. Rather, SBRM focuses on a collaborative and comprehensive sector-wide effort to protect the transportation network as a whole to augment the specific asset protection planning that is currently underway. In most cases, the efforts of the sector stakeholders will not change; however, their appreciation of how those efforts fit within the overall sector risk posture will be significantly enhanced. Introducing SBRM is a first step toward integrating a systems view with the asset-based risk management currently underway.

The eight-step SBRM process, outlined in sections 3, 4, and 5, illustrates three distinct areas of focus to achieve this aim:

- What are we focusing on?
- How do we better understand risk?
- What do we do to manage the risk?

Additionally, the SBRM will help the sector members better understand the true system-wide impact and key interdependencies contained throughout the sector in planning against a terrorist attack or natural disaster. Building on Federal, State, regional, local, and private sector programs and initiatives currently in place, this robust risk management approach entails a continuous process of managing risk through a series of actions, including setting strategic goals and objectives, assessing and quantifying risks, evaluating alternative security measures, selecting which mitigation options to undertake, and implementing and monitoring countermeasures. The SBRM methodology builds on asset-based approaches and is inclusive of current programs and initiatives.

Sector Interdependencies

The Transportation Systems Sector has significant interdependencies with many of the other critical infrastructure sectors. For instance, the Transportation Systems and Energy sectors directly depend on each other to move vast quantities of fuel to a broad range of users and to supply the fuel for all types of transportation. In addition to cross-sector interdependencies, interdependencies and supply chain implications are among the various sectors and modes that must be considered. For example, interdependencies were evident during the aftermath of Hurricane Katrina, where damaged critical infrastructure (pipelines, levees, highways, etc.) disrupted government activities and interrupted commerce flows showing that key interdependencies and supply chain implications must be viewed from a systems-based perspective as opposed to single points or independent assets.

GCC/SCC Structure and Collaboration

The NIPP requires each sector to implement a Sector Partnership Model (SPM) by establishing GCCs, consisting of Federal agencies with sector-specific security responsibilities, and SCCs consisting of private sector organizations, owner-operators, and entities with transportation security responsibilities. The Transportation Systems Sector established an overarching Transportation Systems Sector GCC in January 2006. The Transportation Systems Sector GCC includes the following Federal

agencies with transportation security responsibilities: the DHS, including the Transportation Security Administration (TSA), the United States Coast Guard (USCG), and Office of Grants and Training (G&T); Department of Transportation (DOT); Department of Justice, including the Federal Bureau of Investigation (FBI); and the Department of Defense (DoD). The Transportation Systems Sector GCC is further divided into modal subcouncils (Aviation, Maritime, Mass Transit, Highway, Freight Rail, and Pipeline), which include members from a broad cross-section of government agencies.

The SCCs, following the GCC organizational structure model, are organized, or are organizing, by mode. Membership includes leading associations, as well as owner-operators and other private sector transportation entities with transportation security responsibilities. The SCC currently has efforts underway to organize an overarching Transportation Systems SCC that will interface directly with the Transportation Systems Sector GCC.

These newly formed councils will act in concert to achieve the sector's goals and objectives and continuously refine the sector's security posture through the SBRM process. Both the Transportation Systems Sector GCC and Transportation Systems SCC will work collaboratively to share security information and develop sector-wide approaches to formulating and approving sector priorities, countermeasure programs, and other decisions.

Modal Implementation Plans

As stated above, the Transportation Systems Sector is divided into six modes, each with different operating structures and approaches to security. As required by Executive Order 13416, Strengthening Surface Transportation Security, the Transportation Systems SSP includes modal implementation plans or *modal annexes* that detail how each distinct mode intends to achieve the sector's goals and objectives using the SBRM approach. Separate classified versions of all surface modal implementation plans will be developed as directed by Executive Order 13416. In developing the modal implementation plans, each modal GCC and SCC was required to collaborate in developing an implementation plan that achieves the sector's goals and objectives and identifies the following: cost-effective security programs and initiatives; current industry effective practices; security guidelines, requirements, and compliance/assessment processes; available grant programs; areas for security improvement; and a process to establish metrics for determining security effectiveness and progress toward achieving the sector's goals and objectives. Within each mode, significant actions have already been undertaken to improve the sector's risk profile. These actions include implementing industry security programs and initiatives, expanding customer awareness programs, increasing the number and visibility of security personnel, and upgrading security technology.

DHS CI/KR Protection Annual Report

The Sector CI/KR Protection Annual Report (due every July 1) is an annual requirement of the NIPP in which each sector analyzes the National Risk Profile to identify and determine applicable CI/KR security priorities. The DHS subsequently incorporates priority and resource information from all 17 CI/KR sectors' annual reports to develop an umbrella National CI/KR Protection Annual Report (an overview of the annual report analysis and process is discussed in the 2006 NIPP, pp. 93-96).

The Transportation Systems Sector CI/KR Annual Report that is developed will feed into the National CI/KR Protection Annual Report.

In addition to developing and maintaining a Transportation Systems SSP that supports the NIPP goal and supporting objectives, TSA and USCG, as the Sector-Specific Agencies (SSAs) for the Transportation Systems Sector, in partnership with the SCC and GCC, will determine sector-specific priorities and requirements for CI/KR protection. TSA and USCG will submit these priorities and requirements, along with resource needs, to the DHS in the Transportation Systems Sector Annual Report to allow for a more comprehensive National CI/KR Protection Annual Report.

The annual report will provide:

- Updated sector priorities and goals for CI/KR protection that reflect the current and future-based security status of the Transportation Systems Sector;
- Transportation requirements for CI/KR protection initiatives and programs that are prioritized based on risk and overall protective value; and
- Gap analysis denoting where security programs are lacking and where additional resources are potentially needed.

Appropriations and budgeting projections for NIPP-related CI/KR funding based on the sector's goals and objectives will be included in the SSA budget request as part of the Federal budgeting process.

Intelligence Efforts

One of the key elements influencing sector risk management is intelligence. The sector recognizes the importance of having real-time, credible intelligence information from Federal, State, and local intelligence-gathering entities. Again, looking at recent terrorist events in particular, the foiled plot in the United Kingdom demonstrates the value and necessity of aggressive intelligence and investigative activities. The DHS, through the Office of Intelligence and Analysis, has integrated their efforts with the United States Intelligence Community to ensure continual situational awareness. These offices develop intelligence products and informational materials that inform the efforts of Federal decisionmakers, system operators, and security officials. The concerted effort aims to track potential threats, disrupt development, and focus security resources and activities, as necessary, for detection, deterrence, and prevention. The sector recognizes the importance of private industry integration into the full intelligence cycle, consisting of private industry's intelligence requirements, tasking, analysis, and dissemination. Therefore, the sector will consider establishing a joint GCC/SCC intelligence working group to better coordinate and integrate intelligence efforts with the private sector.

Challenges for the Transportation Systems Sector

The Transportation Systems Sector faces difficult challenges that the sector members must address together. Implementing a sector-wide SBRM approach will provide the mechanism to not only identify SROs, but also to improve resource allocation and security program implementation decisions. However, the sector must resolve additional challenges as it moves forward with security planning efforts, such as: (1) how the Transportation Systems Sector's SSAs—TSA and USCG[137] — can manage the anticipated challenges in preparing future annual reports due to differences in the agencies' budgeting and resource allocation process; (2) how the sector can coordinate response and recovery planning and activities; (3) how the sector can determine, coordinate, and deploy effective research and development initiatives; and (4) how progress in fortifying the sector's security posture and achieving the stated goals and objectives can best be measured.

To address the latter two challenges, the Transportation Systems Sector GCC established a Research and Development (R&D) Working Group to begin coordinating Research, Development, Test, and Evaluation (RDT&E) efforts across the sector. It is envisioned that the R&D Working Group will be comprised of leading R&D experts throughout the Federal Government and the private sector community. Their purpose will be to identify, develop, and prioritize specific R&D security needs through available and proposed technologies. In addition, a Joint Measurement Working Group has been developed to include government and private sector measurement professionals. This group will begin efforts to address the inherent difficulties in measuring and assessing the performance of security solutions by developing measurement approaches and specific metrics to measure progress and transportation security performance. Measurements are not readily applicable in the ways that, for instance,

[137] The USCG, as the SSA for the Maritime Mode, will work within its own budget cycle to provide justifications and execution plans for its security programs. As a multi-mission service, the USCG's assets are used to meet requirements from across its 11 federally mandated mission-programs, one of which is Ports, Waterways, and Coastal Security. The USCG does not have a program dedicated to infrastructure protection, but is able to extrapolate and infer degrees of effort that contribute to infrastructure protection, and will use such methods in its approach to CI/KR risk management and the CI/KR Annual Report.

corporations measure financial performance. Therefore, measurements do not necessarily need to be quantitative. However, sector measurement targets should be specific enough so that reasonable judgments can be made on whether the objectives have been attained.

Another key challenge is the ability to share security information through effective communication tools and mechanisms. The sheer number of stakeholders involved in securing the transportation network can lead to communication disruptions, duplication of efforts, and confusion about roles and responsibilities. As mentioned, the sector has already embraced the NIPP SPM by establishing GCCs and SCCs that provide the framework through which government (Federal, State, local, and tribal) and private sector entities can effectively communicate, coordinate, and collaborate on the sector's security priorities and strategic way forward.

Implementation

The most important aspect of a strategic plan is implementation. As the sector collectively moves forward in securing the Nation's CI/KR, sector stakeholders must work together to implement the sector's strategies and an SBRM approach to drive protection programs and initiatives identified in each mode-specific plan. The Transportation Systems SSP and modal implementation plans are evolving documents that should be updated annually to reflect the continuation of agreements, changes in legislation, or changes in the sector's security posture.

1. Sector Profile and Goals

1.1 Introduction

The Transportation Systems Sector-Specific Plan (SSP) is one of the 17 sector plans required by the National Infrastructure Protection Plan (NIPP), which implements the requirements of Homeland Security Presidential Directive 7 (HSPD-7), Critical Infrastructure Identification, Prioritization, and Protection (December 13, 2003). Under HSPD-7, the Nation's critical infrastructure and key resources (CI/KR) are organized into sectors with certain Federal agencies designated as Sector-Specific Agencies (SSAs). These agencies are responsible for coordinating the protection activities of the sectors' security partners to prepare for and respond to threats that could have a debilitating effect on security or economic well-being. The Department of Homeland Security (DHS) is the SSA for the Transportation Systems Sector. The Secretary of Homeland Security has assigned this responsibility to the Transportation Security Administration (TSA) and the U.S. Coast Guard (USCG) for the maritime mode of the Transportation Systems Sector. The DHS, through TSA and the USCG, in collaboration with the Department of Transportation (DOT) and its modal administrations, and in close cooperation with their Federal, State, local, tribal, and private industry security partners, shares the responsibility for developing, implementing, and updating the Transportation Systems SSP and the supporting modal implementation plan annexes.

The Transportation Systems SSP combines the contributions of the sector's security partners in a sector-wide approach to managing the security risks within and across the transportation modes. Although the principal focus of the Transportation Systems SSP is on risk associated with terrorist threats and resilience, strategies discussed are also applicable to natural disasters and manmade hazards. The Transportation Systems SSP and its modal annexes explain how the Transportation Systems Sector will improve the security of its CI/KR assets, systems, networks, and functions that provide the vital services essential for the Nation's security, economic vitality, and way of life.

The national effort to improve CI/KR security also must conform to several other key Presidential Directives and Executive Orders. In conformance with HSPD-5, Management of Domestic Incidents, domestic incidents will be managed under the principles set forth in the National Response Plan (NRP) and the National Incident Management System (NIMS). The NRP explains how Federal, State, and local agencies will respond to all types of hazards. The NIMS organizational approach provides the doctrinal basis for determining and coordinating the resources necessary to manage incidents of all sizes and complexity. The NRP and the NIMS are currently undergoing a review process. This revision, fully engaging all levels of sector stakeholders, will determine the roles and responsibilities for response and recovery. In the meantime, the sector will begin the process of establishing a Response and Recovery Working Group (R&RWG) to determine how its efforts can be integrated into the NRP/NIMS review process. The National Preparedness Goal developed under HSPD-8, National Preparedness, provides specific objectives to ensure that communities are prepared for natural or human-caused disasters and terrorist attacks. Maritime mode security is specifically addressed in HSPD-13, National Strategy for Maritime Security, which underscores the importance of securing the maritime domain, developing a comprehensive national strategy, and ensuring effective and

efficient implementation of strategies. As directed in Executive Order 13416, Strengthening Surface Transportation Security, the Secretary of Homeland Security leads the efforts for protection of the surface transportation modes by the facilitation and implementation of a comprehensive, coordinated, and efficient security program.

To address the threat of a novel influenza virus with pandemic potential, the President, on November 1, 2005, announced the National Strategy for Pandemic Influenza (NSPI), which outlines the approach that the U.S. government will take to prepare for and respond to an influenza pandemic. It also articulates the expectation that non-Federal entities will prepare themselves and their communities.

To translate the NSPI into effective actions, an accompanying Homeland Security Council (HSC) Implementation Plan for the national strategy identifies major roles and responsibilities for Federal departments and agencies. While the Department of Health and Human Services (DHHS) is the lead for public health, the DHS, with the lead for domestic incident management, and particularly border and transportation security, plays a pivotal role in the execution of the national response. Further planning coordination occurs between the DHS and the DHS component agencies and their Federal partners, many of which are outlined in the Transportation Systems SSP, on domestic and international transportation-related issues, specifically the departments of Transportation, State, and Defense.

Each Federal department and agency is responsible for creating and maintaining a pandemic influenza contingency plan. These plans include provisions for the protection of employees, the maintenance of essential functions and services, communications with stakeholders, and the manner in which the department will execute its responsibilities in support of the Federal response to a pandemic, as described in the HSC Implementation Plan.

The HSC Implementation Plan, which contains more than 300 action items to prepare for and respond to a pandemic, dedicates a section to the protection and continuity of CI/KR during a pandemic, including transportation. The Implementation Plan outlines several mechanisms and timelines for engaging stakeholders and providing guidance for their own contingency plans in support of the national response.

1.2 Sector Profile

The Nation's transportation network is a vast, open, accessible, interconnected system with as much as 85 percent of the transportation infrastructure in the United States owned by the private sector. The sheer size and capacity of this sector, which moves, distributes, and delivers millions of passengers and goods each year, makes it a highly attractive target for terrorists and a challenge to secure.

The Transportation Systems Sector is segmented into six key subsectors, or modes, which operate independently within both a regulated and non-regulated environment, yet are also highly interdependent. Such interdependence is a defining characteristic of the transportation system. The six modes—Aviation, Maritime, Mass Transit, Highway, Freight Rail, and Pipeline—all contribute to transporting people, food, water, medicines, fuel, and other commodities. The combined efforts of the modes play an important role in maintaining the public health, safety, and economic well-being of our Nation. Yet, each does so with unique characteristics, operating models, responsibilities, and stakeholders.

1. **Aviation** includes aircraft, air traffic control systems, and approximately 450 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.
2. **Maritime** includes the wide range of water-faring 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 Exclusive Economic Zone to secure, and intermodal landside connections, which allow the various modes of transportation to move people and goods to, from, and on the water.

3. **Mass Transit** includes multiple-occupancy vehicles, such as transit buses, trolleybuses, vanpools, ferryboats, monorails, heavy (subway) and light rail, passenger rail (including both commuter rail and long-distance rail), automated guideway transit, inclined planes, and cable cars, designed to transport customers on regional and local routes.

4. **Highway** encompasses more than 4 million miles of roadways and supporting infrastructure. Vehicles include automobiles, buses, motorcycles, and all types of trucks, trailers, and recreational vehicles.

5. **Freight Rail** consists of hundreds of railroads, more than 143,000 route-miles of track, more than 1.3 million freight cars, and roughly 20,000 locomotives.

6. **Pipeline** includes vast networks of pipeline that traverse hundreds of thousands of miles throughout the country, carrying nearly all of the Nation's natural gas and about 65 percent of hazardous liquids, as well as various chemicals.

As mentioned previously, each mode of the Transportation Systems Sector, having different security and operating environments, has developed separate modal implementation plans that are included as annexes to the Transportation Systems SSP. The plans detail the characteristics of the mode, including approaches to security, industry effective practices, guidelines, assessments, and regulations. In parallel with developing the Transportation Systems SSP, the plans explain how each mode will incorporate sector goals into modal security programs.

1.2.1 Cross-Sector Dependencies

There are many dependencies and interdependencies between the various CI/KR sectors. Virtually every sector is dependent, to some degree, on the Energy, Communications, and Transportation Systems sectors. In addition, because critical sectors have different and potentially competing interdependencies, it is vitally important to determine key relationships to gain a better understanding of the overall complexities when undertaking planning and policy initiatives for critical infrastructure protection (CIP). Key dependencies are those that, if interrupted, could significantly impact the performance of the transportation system and its overall resilience.

As the following examples demonstrate, CI/KR sectors not commonly associated with transportation will be significantly impacted by a major disruption in one or more of the transportation modes.

- The Energy Sector requires coal, crude oil, petroleum products, and natural gas that are transported by ship, barge, pipeline, rail, and truck.
- The Defense Industrial Base uses the Nation's air, maritime, rail, and highway networks to move materiel in support of military operations.
- The Banking and Finance Sector and Government Facilities Sector rely on mass transit systems in large urban areas for employees to access the workplace.
- 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.
- The manufacturing and commercial sectors move goods and services across the entire transportation network utilizing all transportation modes.

The integrity of the Transportation Systems Sector is also directly dependent on the efforts of other sectors.[138]

- The Energy Sector produces fuels to power transportation systems.

[138] Cross-sector working groups and simulation models via the National Infrastructure Simulation and Analysis Center (NISAC) (e.g., Critical Infrastructure Protection/Decision Support System (CIP/DSS)) will be used to further explore these interdependencies.

- The Information Technology Sector is essential in the transmission of information necessary for the efficient operation of the transportation network.

In addition to cross-sector interdependencies, the Transportation Systems Sector must pay particular attention to interdependencies among the transportation modes. Those issues that affect more than one mode will be given special consideration, recognizing that many assets serve more than one mode.

As with the traditional aspects of the transportation network, interdependencies also exist between cyber assets, people, and the facilities in which they reside. To identify and prioritize these dependencies, sector members are encouraged to perform an interdependency analysis, which government agencies, private companies, and universities have developed. TSA and USCG, as the SSAs, will help sector members identify a methodology that meets their needs.

1.3 The Transportation Security Environment

Like many other critical infrastructure sectors, the Transportation Systems Sector faces a dynamic landscape of potential natural disasters, accidents, and terrorist attacks. The terrorist threat poses special challenges. While terrorists may rely on a distinct set of attack methods, they can adjust their attack strategies based on past responses. As a result, unlike natural disasters or accidents, the time and place of terrorist attacks cannot easily be predicted by just evaluating historical events. Modes of transportation have been used in terrorist attacks not only in New York and Washington, DC, on September 11, 2001, but also in London, Madrid, and Mumbai, India.

The Transportation Systems Sector is highly complex because of a number of reasons. One reason is sheer scale—the sector is composed of hundreds of thousands of assets, links, and nodes spread across the six modes. Some assets, such as airports or rail yards, are stationary. Others, such as hazardous materials (HAZMAT) trucks or commercial airplanes, are mobile and may be used as weapons, as well as targets. These assets are widely distributed geographically, in both rural and urban areas, covering all 50 States and Territories.

Secondly, the Transportation Systems Sector consists of numerous and diverse stakeholders, including Federal, State, and local government agencies, as well as private owner/operators. Owner/operators across the modes may face different decision incentives and constraints.

A third reason for the complexity that characterizes the Nation's transportation network is interconnectedness and supply chain implications among the assets and systems that comprise it. The security challenge faced by the 21st century transportation community is due, in large part, to the interconnected, interdependent network that has been created to meet the demands of the economy and of the citizens. Over the past two decades, the sector, like most other infrastructures, has expanded and altered its business models on a global scale to take advantage of the so-called "network effect."[139] While these changes have significantly enhanced the efficiency and effectiveness of the sector, they have also resulted in a more complicated operating model. The result is a transportation network that becomes more and more complex and interdependent each year.

These insights are key to understanding why the sector's mission is to enhance transportation security while maintaining the free flow of commerce. Terrorists have sought to inflict damage that is disproportionate to their efforts by attacking parts of the network that will lead to nonlinear consequences, such as a cascading failure. Additionally, terrorist threats are adaptive and dynamic in that security applied to one element of the transportation network could cause terrorists to shift their attention to other parts of the system. Therefore, the sector must simultaneously seek to improve security while minimizing the negative impact of countermeasures to ensure that macro (emergent) patterns of commerce in the transportation system are not disrupted.

[139] A characteristic that causes a good or service to have a value to a potential customer dependent upon the number of customers already owning that good or using that service.

1.4 Sector's Approach to Risk Management

An environment of complexity and uncertainty presents the Transportation Systems Sector with a set of challenging and sometimes conflicting decisions on how best to increase the security and resilience of the Nation's transportation network. Various stakeholders throughout the sector are actively developing methods to improve operational security and overall resilience. However, increased emphasis needs to be placed on understanding the evolving risk-based approach to security.

The Secretary of Homeland Security, Michael Chertoff, has described his vision for risk-based decisionmaking, stating *"We must manage risk at the homeland security level. That means developing plans and allocating resources in a way that balances security with freedom when calculating risks and implementing protections."*[140]

As part of their day-to-day risk management efforts, stakeholders within the sector secure their organizations from the specific risks that threaten them. The DHS and other government entities provide the private sector with threat warning, incident reporting, and analysis whenever appropriate. Such information is critical to the sector's operational and tactical planning and implementation. Depending on the threat information, the sector may choose to adjust their operational and tactical efforts.

Due to the interconnectedness and supply chain implications of systems within the transportation network and the possibility of cascading effects from a major event, it is important to focus sector-wide efforts on strategic risks. Strategic risks are those that impact the entire sector, threatening disruption across multiple stakeholder communities. The consequences of strategic risks can also cross multiple sectors and can have far-reaching, long-term effects on our national economy, natural environment, or public confidence. Examples of strategic risks to the Transportation Systems Sector include:

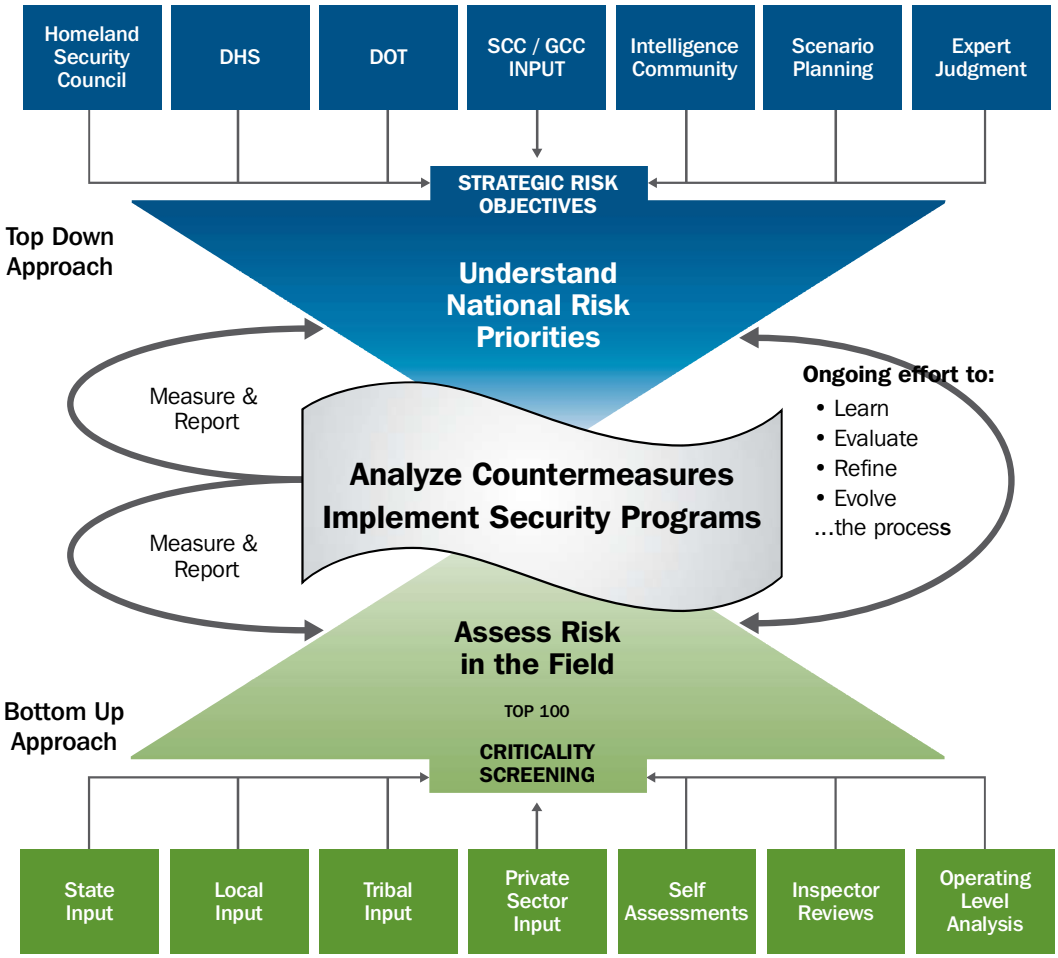
- Disruption of a mega-node[141] in the transportation network (large-scale impact on national security);
- Use of a component of the transportation network as a weapon of mass destruction (WMD) (terrorism event leading to loss of life and public confidence); and
- Release of a biological agent at a major passenger facility, such as a rail station, ferry terminal, or hub airport (terrorism event affecting national public health and safety).

Stakeholders throughout the sector have been and continue to be actively developing methods to improve their operational security and overall resilience. However, since the Transportation Systems Sector is segmented by individual modes, an increased emphasis is needed on a risk-based approach across the entire transportation spectrum. The sector's risk management approach reflects a combined top-down and bottom-up effort. Figure 1-1 illustrates the dynamic and collaborative risk assessment process and those involved in determining which risks will be identified, analyzed, prioritized, and addressed.

[140] Secretary of Homeland Security, Michael Chertoff, address at The George Washington University's Homeland Security Policy Institute, March 16, 2005.

[141] A mega-node refers to a single point of possible failure or bottleneck, at which multiple modes of transportation intersect, with the potential for wide-ranging disruptions and losses. An example of a mega-node is New Orleans, where all transportation modes meet and exchange goods and people. As seen in 2004, a disruption at this mega-node had wide-ranging effects on fuel, food, the movement of people, etc.

Figure 1-1: Integrated Top-Down, Bottom-Up Risk Assessment Cycle



1.4.1 NIPP Risk Management Framework

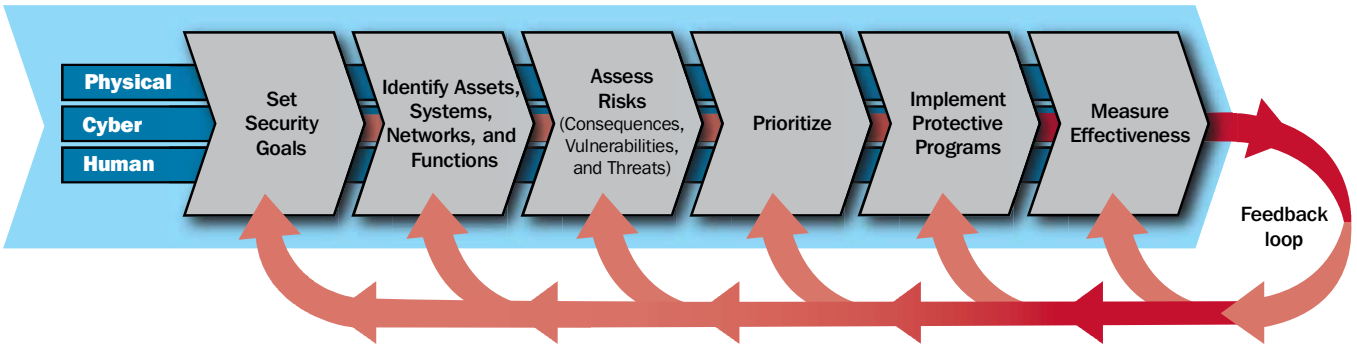
The NIPP identifies an overarching goal:

Build a safer, more secure, and more resilient America by enhancing protection of the Nation's CI/KR to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them; and to strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency.

This goal also includes a risk management framework to support it. This risk management framework allows risk-reduction and protection measures to be applied where they offer the most benefit. Once security goals are set, the NIPP framework involves five subsequent key steps: (1) identifying CI/KR assets across the 17 sectors; (2) identifying and assessing risks; (3) normalizing, analyzing, and prioritizing study results; (4) implementing protective programs; and (5) measuring effectiveness.

Figure 1-2 shows the risk management framework outlined in the NIPP for developing each sector's security program. The expected output of this process is a set of sector-specific strategies to protect assets and systems. The Transportation Systems SSP builds directly upon this model, using it as the basis for its organization and as a starting point for its Systems-Based Risk Management (SBRM) approach.

Figure 1-2: NIPP Risk Management Framework



The Transportation Systems Sector recognizes the value of the NIPP framework for Federal, State, local, tribal, and private participants and is aware that each mode has unique characteristics, business models, system and asset classes, and sub-modes. Also, the sector members understand they must work together to achieve a consistent, sustainable, effective, and measurable security posture that preserves public safety and efficient commerce with minimal restriction of movement to cargo and people.

1.4.2 Systems-Based Risk Management Framework

To achieve the security posture described in the previous section, the Transportation Systems Sector developed a collaborative methodology that applies a systems-based approach to managing threats, vulnerabilities, and consequences across the physical and cyber domains. As the agency responsible for managing strategic risks across the National Transportation System (NTS), TSA, as the SSA, not only looks at asset-level risk, but system-level risk as well. An asset-level risk is the combination of threat, vulnerability, and consequences for individual assets. System-level risks are those risks associated with combinations of assets, their relationships, their functions, and their emergent properties and characteristics. Because individual assets are part of a larger interconnected system, the consequences of a system-level failure can far exceed the consequences associated with a single asset. The SBRM approach accounts for network vulnerabilities and potential ripple effects—conditions created because of the interconnectedness and interdependence of transportation assets, systems, and functions nationwide—and augments asset-based risk assessments by providing insight into how the loss of individual assets or a collection of assets will impact the overall transportation system. This approach will enable the sector to better determine critical transportation systems and assets, and prioritize these systems and assets against limited resources (this approach is discussed further in section 3, Assess Risks).

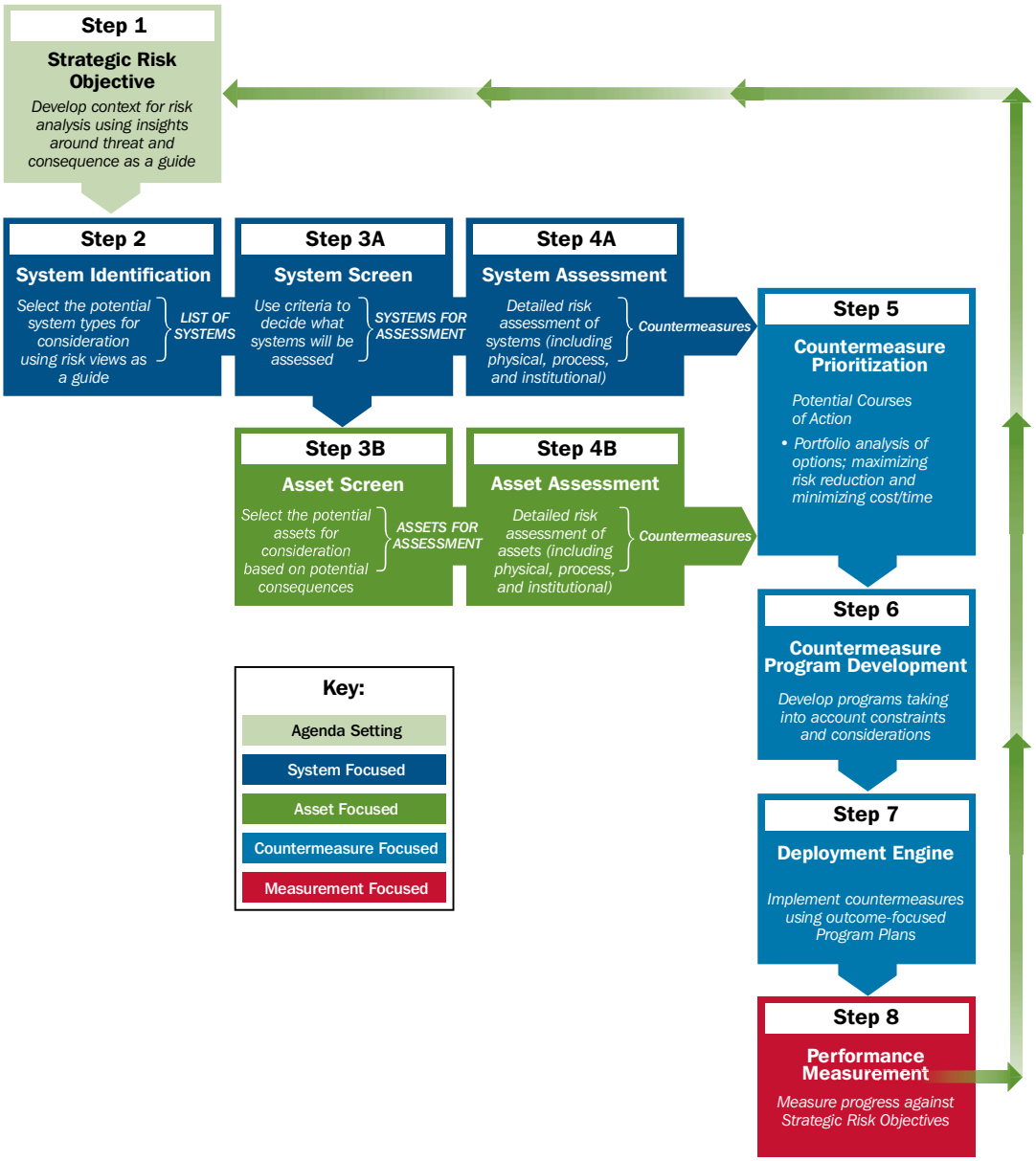
The SBRM, shown in figure 1-3, links strategic goals and resulting performance to help meet the objectives as stated in this document and the NIPP. The SBRM process sets a strategic course for sector-wide risk management, yields strategic counter-measures, and does not specifically address operational or tactical planning.

The ability to manage risk by providing an integrated, structured, repeatable, adaptable process allows the Transportation Systems Sector to improve its risk management process over time. This process does not replace current methodologies and practices. Rather, it is an inclusive framework designed to use current processes and enrich the analysis of risk via a systems view.

Figure 1-3 illustrates the SBRM process that results in a comprehensive view of strategic risks in the transportation network. This risk management approach will identify specific strategic risk objectives (SROs) that will focus the development of a portfolio of asset- and systems-based risk management options. SROs, developed by both public and private industry leaders, are statements that establish a specific, measurable, realistic, attainable target that, when achieved, will improve the sector's risk profile. They set the target for required performance in light of specific consequences that span multiple stakeholders,

transportation systems, or critical infrastructure sectors. Consequences can have nationwide implications to national security, health and human safety, the economy, the environment, or public confidence. To understand the evolution of those SROs and the sector goals that support them, which are laid out in section 1.5, the process that developed those SROs and the SBRM process that will update them in future iterations must be described.

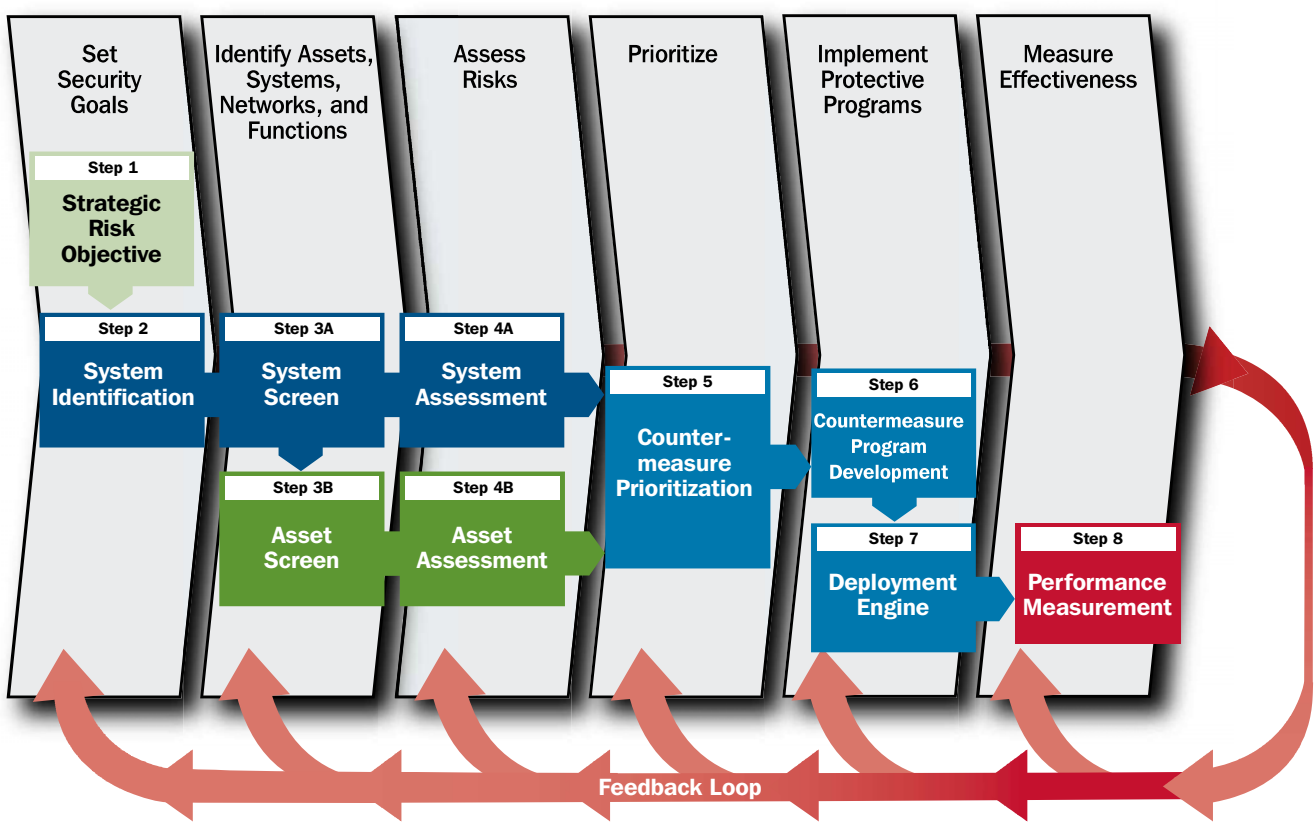
Figure 1-3: Summary of Systems-Based Risk Management Process[142]



[142] As SSAs, TSA and USCG, in collaboration with DOT, are the leads for implementation of the SBRM process in cooperation with government and private sector partners.

As shown above and explained in further detail in sections 3, 4, and 5, this plan seeks to ensure that the Transportation Systems Sector has the key capabilities required to manage strategic risks by building upon and extending current asset-based approaches. The SBRM process is an expansion of the six steps of the NIPP risk management framework detailed in figure 1-2. It focuses on three distinct areas: what we are concerned with (SROs), how the risk is understood using analytical evaluations, and how to manage risk by determining which countermeasures to invest in and measure. Figure 1-4 shows the relationship between the NIPP risk management framework and the Transportation Systems Sector's SBRM process.

Figure 1-4: NIPP Risk Management Framework/Systems-Based Risk Management Process



1.5 Transportation Systems Sector Security Goals and Objectives

The sector's security goals and objectives provided below are consistent with the goals outlined in the President's National Strategy for Homeland Security and the joint DHS and DOT National Strategy for Transportation Security (NSTS). These goals and objectives represent the initial view of the sector's security partners regarding strategic approaches for managing sector risk and include a range of flexible, layered, and unpredictable security programs that address the sector's risk-based priorities. The goals are supported by more specific and measurable objectives that indicate sector security priorities.

Initially, the sector vision statement, goals, and objectives were developed by the SSAs (TSA and USCG) and their Federal security partners (e.g., DOT, the DHS Office of Grants and Training (G&T), Customs and Border Protection (CBP), other agencies within the DHS, the Department of Defense (DoD), and the Department of Justice (DOJ)), drawing from existing national transportation security plans and strategies. From this initial effort, the Transportation Systems Sector modal Government

Coordinating Councils (GCCs) and Sector Coordinating Councils (SCCs) provided vital comments and suggestions that enabled completion of the sector vision statement, as well as a set of goals and objectives.

The vision statement sets the stage for developing sector-specific security goals that are aligned with national goals. These strategic sector goals are needed to accomplish the sector's mission, as described below. Each stated goal is supported by a set of descriptive objectives.

Vision Statement for the Transportation Systems Sector

Our vision is a secure and resilient transportation network, enabling legitimate travelers and goods to move without undue fear of harm or significant disruption of commerce and civil liberties.

Mission Statement for the Transportation Systems Sector

Continuously improve the risk posture of the Nation's transportation system.

The Transportation Systems Sector's mission, to continuously improve the risk posture of the national transportation system, is the foundation of the risk framework. The future development of the sector's goals and objectives will be informed by the SBRM process and driven by the formulation of SROs through the GCC/SCC framework.

Goal 1: Prevent and deter acts of terrorism using or against the transportation system.

Terrorist attacks may seek to directly disrupt transportation systems or they may use transportation systems to carry out larger attacks against the American people. The primary goal of the Transportation Systems Sector is to prevent and deter criminal and terrorist attacks before they happen without disrupting the free flow of commerce or compromising civil liberties.

Objectives

- Implement flexible, layered, and effective security programs using risk management principles. (Security measures need to be developed and established on the basis of risk analyses and should provide multiple opportunities to prevent an attack; should also continually evolve, introducing elements of uncertainty and unpredictability into an adversary's planning and surveillance efforts; and should be adaptable to different modes and threats in order to increase their robustness in the face of a dynamic and learning enemy.)
- Increase vigilance of travelers and transportation workers. (By having an active role in identifying and reporting suspicious activity, the traveling public and transportation workers can serve as force multipliers to Federal, State, and local law enforcement efforts.)
- Enhance information and intelligence sharing among Transportation Systems Sector security partners. (The development of relationships and improved technology can provide Federal, State, local, tribal, private sector, and international transportation security partners with a platform to share and exchange security information, such as threats, best practices, lessons learned, or other experiences to improve transportation security.)

Goal 2: Enhance resilience of the U.S. transportation system.

The resilience of a transportation system 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 response and recovery activities.

Objectives

- Manage and reduce the risk associated with key nodes, links, and flows within critical transportation systems to improve overall network survivability. (Many transportation systems contain a small number of critical assets that, if attacked, could result in catastrophic failure. These assets can take the form of a node, a link, or a flow. Security strategies must be identified to shift the threat away from these critical assets via risk management. The preferred risk management technique is to reduce risk; although, in certain cases, hedging, transferring, or even accepting the risk may be acceptable and warranted. If it is desired to reduce the risk, various approaches could be used, including deterrence and vulnerability reduction measures (as identified in Goal 1), or consequence mitigation measures, including hardening and increasing the redundancy of the key assets.)
- Enhance the capacity for rapid and flexible response and recovery to all-hazards events. (Response and recovery activities traditionally include first-responder actions and the plans, training, and exercises that support them. Response and recovery activities can also include pre-establishing re-routing procedures, emergency suppliers, and evacuation processes.)

Goal 3: Improve the cost-effective use of resources for transportation security.

Minimizing unnecessary duplication of efforts, improving coordination, and aligning resources to the highest risks all help the Transportation Systems Sector improve the cost-effective use of resources.

Objectives

- Align sector resources with the highest priority transportation security risks using both risk and economic analyses as decision criteria. (The Transportation Systems Sector will collectively define its highest risks and work together to ensure that resources are appropriately aligned against them.)
- Ensure robust sector participation in the development and implementation of public sector programs for CI/KR protection. (In order to ensure that Federal, State, local, and private sector efforts are harmonized, the Transportation Systems Sector will utilize the GCC/SCC framework to jointly develop and implement security programs.)
- Ensure coordination and enhance risk-based prioritization of Transportation Systems Sector security Research, Development, Test, and Evaluation (RDT&E) efforts. (There are various research and development (R&D) efforts throughout the Federal Government and private sector. To avoid unnecessary duplication of efforts and to spur collaborative efforts, the GCC and SCC structure will be used to coordinate these efforts.)
- Align risk analysis methodologies with NIPP Baseline Criteria for assessment methodologies. (The NIPP Baseline Criteria states that risk analysis methodologies should be credible, documented, transparent, reproducible, and accurate, and they should enable sector leaders to make sound, cost-effective security decisions.)

1.6 Value Proposition

The Transportation Systems SSP is valuable to the American people if it enables the responsible public and private officials—the sector's security partners—to implement programs and activities that create a secure and resilient transportation network as described in the sector's vision statement. The sector's security partners should recognize the Transportation Systems SSP as the blueprint for building the protective end-state, as expressed in the vision statement. With a common understanding of the transportation network and a common application of the sector's risk management process, the security partners can develop cogent recommendations for changes in public policy. To address TSA's mission, the commitment and participation of the sector's many diverse stakeholders is vital to prevent, protect against, respond to, and recover from potential terrorist attacks and other incidents. High levels of communication and coordinated action are required, often within very short periods of time.

Each year, the Federal executive agencies receive billions of dollars, in aggregate, for security programs, grants, and R&D of homeland security initiatives. These agencies must make programmatic decisions on distributing funds and make proposals for

future appropriations. Active participation in the development and implementation of the Transportation Systems SSP, through the GCC/SCC framework, affords stakeholders the opportunity to contribute significantly to shaping the Federal Government's risk-based decisionmaking.

1.7 Security Partners

The term "security partners" as used in the NIPP refers to the entire landscape of participants in the infrastructure protection planning process and includes all levels of government (Federal, State, Territorial, local, and tribal), regional organizations, international partners, and private sector owners and operators. The Transportation Systems Sector partnership model[143] will facilitate effective coordination between government and the private sector. Through this partnership, all sector security partners have roles and responsibilities in developing a robust SSP that is representative of their interests.

1.7.1 The Transportation Systems Sector-Specific Agencies

TSA was assigned responsibility as the SSA for the Transportation Systems Sector. The USCG was designated the SSA for the Maritime mode. TSA and USCG have the responsibility to implement HSPD-7 through the NIPP Sector Partnership Model.

1.7.2 NIPP Sector Partnership Model for the Transportation Systems Sector

The DHS has the responsibility for developing a comprehensive national plan for securing CI/KR and for recommending "measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other agencies of the Federal Government and in cooperation with State and local government agencies and authorities, the private sector, and other entities." The NIPP calls for implementing a sector partnership model as the primary organizational structure for coordinating and implementing CI/KR efforts and activities. The sector partnership model encourages formation of SCCs and GCCs as security partners to support activities required to implement and sustain the national, as well as sector-specific, CI/KR protection efforts.

Government Coordinating Councils

The primary mission of the GCC is to facilitate the development of comprehensive sector-wide strategies that advance CIP. GCCs may identify gaps in plans, programs, policies, procedures, and strategies, and serve as the forum to work with the private sector to develop, implement, and update each SSP. The designated SSA chairs each GCC, and the DHS Assistant Secretary for Infrastructure Protection is the co-chair. The GCC serves as a counterpart to the SCC for each CI/KR sector and is composed of Federal, State, and local governments, and tribal interests.

The Transportation Systems Sector GCC was formed in early 2006 with the mission "to coordinate transportation security strategies and activities with all its security partners and establish policies, guidelines, and standards, and to develop program metrics and performance criteria for all transportation modes." The Transportation Systems Sector GCC fosters communication across government agencies and between the government and private industry in support of the Nation's homeland security mission. The GCC acts as the counterpart to the private industry-led SCC for transportation to review and develop the sector-wide security programs necessary to protect the Nation's transportation system.

The Transportation Systems Sector GCC includes the following member agencies:

- Department of Homeland Security (TSA, USCG, Infrastructure Protection, and G&T);
- Department of Transportation (DOT);
- Department of Energy (DOE); and

[143] The Sector Partnership Model is the primary organizational structure for coordinating CI/KR efforts and activities as described in the NIPP.

• Department of Defense (DoD).

The Transportation Systems Sector GCC will expand its membership as necessary.

By mid-April 2006, each mode in the Transportation Systems Sector began to develop its own modal GCC structure under the Transportation Systems Sector GCC and began to discuss priorities for joint work with their counterpart SCC. 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 GCC structure includes members from the Transportation Systems Sector GCC, as well as other Federal agencies such as DOJ and the Department of Commerce (DOC) to name a few.

Through the Transportation Systems Sector GCC framework, shown in figure 1-5, Federal Government agencies with transportation security responsibilities are engaged and collaborate with the Transportation Systems SCC to refine and finalize the sector goals, develop the Transportation Systems SSP, and develop a mode-specific implementation plan to achieve the sector's goals. The GCC, working with the SCC, will serve as the integration council to ensure that CI/KR protection activities are accomplished. This may include:

• Structure an effective SBRM approach to identify and prioritize countermeasures within the sector;

• Plan and implement response and recovery activities and communication following an incident or event;

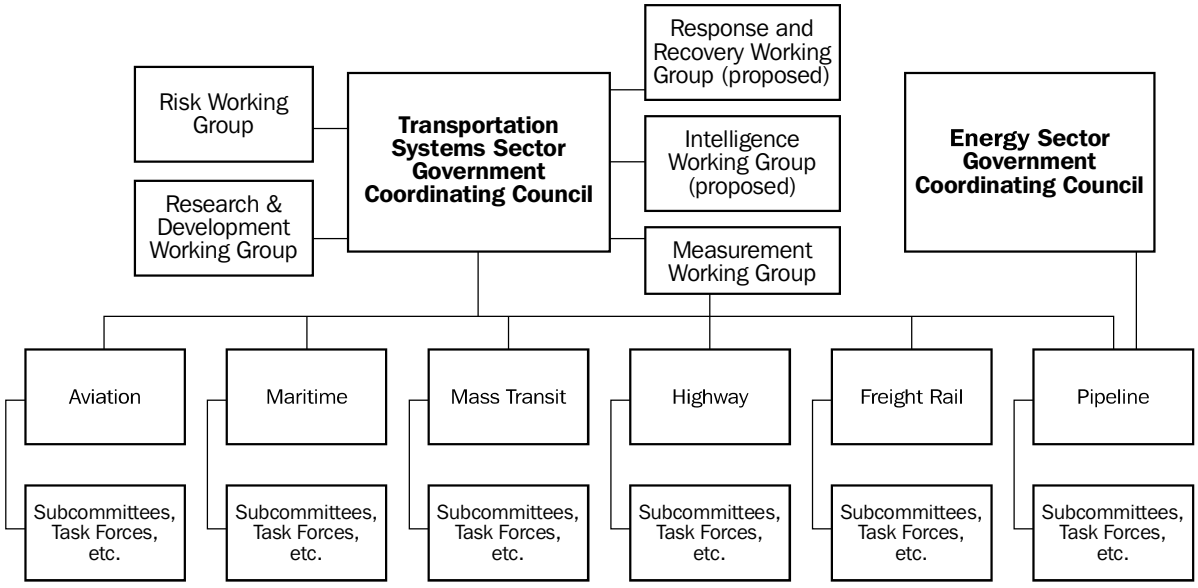
• Share credible intelligence and other relevant security information through communication mechanisms that are appropriate and effective;

• Facilitate the development of security guidelines, standards, regulations, and assessments;

• Identify and implement the information-sharing mechanisms; and

• Work with the SCC to enhance existing working groups and, when necessary, establish additional working groups.

Figure 1-5: Transportation Systems Sector GCC Organization

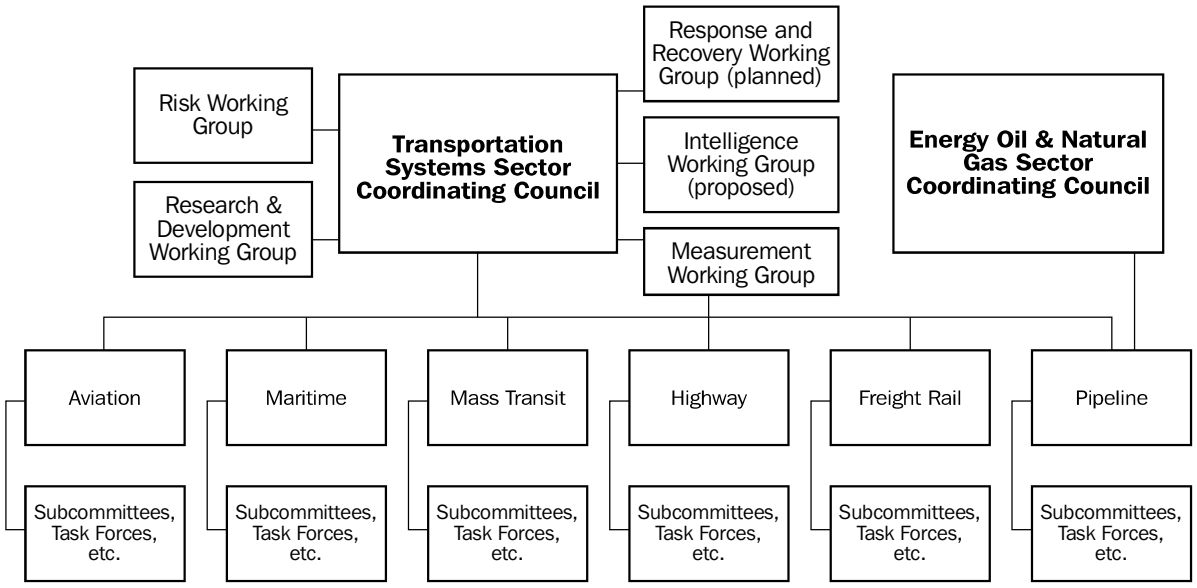


Note: Refer to the Pipeline Modal Implementation Plan (annex F) for more information on the Pipeline GCC.

Sector Coordinating Councils

SCCs are self-formed councils composed of private sector representatives of infrastructure owners, operators, and related trade associations. Through the transportation SCC framework, private sector participants can provide input to the GCC to help refine and finalize the sector goals, develop the Transportation Systems SSP, and develop mode-specific implementation plans and programs to achieve the sector's goals. While the Transportation Systems SCC, shown in figure 1-6 below, is in the process of being organized, modal SCCs for each transportation mode have been established. Once the Transportation Systems SCC is organized and fully functional, membership can be expanded in the future, as necessary.

Figure 1-6: Transportation Systems SCC Organization



Note: Refer to the Pipeline Modal Implementation Plan (annex F) for more information on the Pipeline SCC.

The SCC also plays an important role in providing expertise and leadership in CI/KR protection activities including, but not limited to:

- Contributing to an effective SBRM approach by working in partnership with the GCCs to identify and provide information regarding security measure priorities within the sector;
- Planning and implementing response and recovery activities and communication following an incident or event;
- Sharing information related to best practices, credible threats, risk data, incidents, domain awareness campaigns, etc.;
- Identifying and implementing the information-sharing mechanisms that are most appropriate for their mode (e.g., Homeland Security Information Network (HSIN), Homeport); and
- Working with the GCC to enhance existing working groups and, when necessary, establish additional working groups.

Critical Infrastructure Partnership Advisory Council (CIPAC)

To secure our Nation's most critical infrastructure, the Federal Government and private sector must collaborate to identify, prioritize, and coordinate CI/KR protection, as well as share information about physical and cyber threats, vulnerabilities,

incidents, and potential protective measures and best practices. To facilitate the successful execution of the sector partnership structure and to develop security plans, members of the SCCs and GCCs require an environment where they can discuss sensitive security matters. The 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 CIP issues. The process facilitates the sharing of security 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.

1.7.3 Key Federal Transportation Security Partners

Department of Homeland Security

The DHS's mission is to lead the unified national effort to secure America. The DHS will prevent and deter terrorist attacks and protect against and respond to threats and hazards to the Nation. The DHS will ensure safe and secure borders, welcome lawful immigrants and visitors, and promote the free flow of commerce. A number of offices and agencies within the DHS have responsibilities that directly or indirectly contribute to transportation network security. Additionally, agencies outside of the DHS also have responsibilities and interests in the Transportation Systems Sector.

The following are descriptions of Transportation Systems Sector GCC members.

- **Transportation Security Administration.** TSA was created under the Aviation and Transportation Security Act (ATSA), which gave TSA responsibility for security in all modes of transportation. As part of its security mission, TSA is responsible for assessing intelligence, enforcing security-related regulations and requirements, ensuring the adequacy of security measures at transportation facilities, and carrying out other transportation security responsibilities. Under HSPD-7, TSA was designated as the SSA for the Transportation Systems Sector by the Department of Homeland Security.
- **U.S. Coast Guard.** 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 and waterways, 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, USCG will often act in a first-responder capacity. USCG also serves as the SSA for the Maritime transportation mode. The DHS, with USCG as its executive agent, has the primary responsibility for maritime homeland security, including coordinating mitigation measures to expedite the recovery of infrastructure and transportation systems in the maritime domain, with the exception of DoD installations.
- **Grants and Training.** The Office of Grants and Training 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 acts of terrorism.
- **Office of Infrastructure Protection (IP).** The DHS IP has the overall responsibility for coordinating implementation of the NIPP across the 17 CI/KR sectors; overseeing the development of 17 CI/KR SSPs that outline processes and measures to secure the Nation's CI/KR; providing training and plans for protective measures to assist owners and operators in securing the CI/KR within their control; and helping State, local, tribal, and private sector partners develop the capabilities to mitigate vulnerabilities and identifiable risks to their assets. Through the NIPP Sector Partnership Model (SPM), the DHS IP coordinates security activities to reduce the Nation's vulnerability to terrorist attacks through a unified national approach.
- **Department of Transportation.** DOT has the responsibility for promoting safety, including hazardous materials security, through advocacy, regulation, enforcement, grants, and other means. DOT modal administrations manage many transportation programs that directly affect the protection of critical transportation infrastructure. As stated in HSPD-7, DOT and the DHS will collaborate on all matters related to transportation security and transportation infrastructure protection in order

to balance security requirements with the safety, mobility, and economic needs of the Nation and be prepared to respond to emergencies that affect the viability of the sector.

- **Department of Energy.** As SSA for the Energy Sector, DOE is responsible for ensuring the security of the Nation's energy CI/KR. DOE is a member of the Transportation Systems Sector GCC in its capacity as the lead Federal agency responsible for energy. Energy commodities are transported by pipelines, ships, barge, rail, and tanker trucks—assets and systems that cross over into the responsibility of the Transportation Systems Sector.
- **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 transportation security incident. DoD has equities in the security of the commercial aspects of the Transportation Systems Sector and has policy devoted to the security of DoD shipments. DoD, as a member of the Transportation Systems Sector GCC, will be involved with the collaboration to determine transportation security policies and decisions. Agencies within DoD with transportation security responsibilities appear in appendix 4.

Additional Federal Security Partners

A number of Federal agencies work closely with the sector to ensure its security and the free flow of goods and passengers. Two agencies with direct involvement in transportation security are listed below. Other Federal security partners are listed in appendix 4.

- **Department of Justice.** DOJ acts to reduce criminal and terrorists threats, and investigates and prosecutes actual or attempted attacks on, sabotage of, or disruptions of CI/KR in collaboration with the DHS.
- **Federal Bureau of Investigation (FBI).** The FBI is the principal investigative arm of the DOJ and the lead Federal agency for investigations of terrorist acts or terrorist threats by individuals or groups inside of the United States or directed at U.S. citizens or institutions abroad, where such acts are within the Federal criminal jurisdiction of the United States. Within the Transportation Systems Sector, the FBI will act to reduce terrorist threats, as well as investigate and prosecute actual or attempted terrorist attacks on, sabotage of, or disruption of CI/KR. The FBI will investigate and prosecute general criminal violations within the transportation system as directed by statute.
- **Customs and Border Protection.** CBP plays a key role in transportation security and protects against external threats that seek entry into the United States. CBP accomplishes this wide-ranging responsibility by reviewing and verifying cargo manifests, inspecting containers and persons, patrolling the Nation's land borders, and patrolling airways and marine ports. CBP officers are stationed at airports and seaports as well. CBP is also involved in security efforts pertaining to cross-border rail, trucking, and pipeline transportation.
- **Department of Commerce.** DOC has many component agencies involved with transportation security-related activities, such as the National Institute of Standards and Technology (NIST), the National Oceanic and Atmospheric Administration (NOAA), the National Telecommunications and Information Administration (NTIA), and the Bureau of Industry and Security (BIS). BIS advances U.S. national security, foreign policy, and economic interests for DOC, and plays a critical role in developing, promoting, and implementing policies that ensure a strong, technologically superior defense industrial base. BIS activities include regulating the export of sensitive goods and technologies in an effective and efficient manner; enforcing export control, anti-boycott, and public safety laws; cooperating with and assisting other countries on export control and strategic trade issues; assisting U.S. industry to comply with international arms control agreements; and monitoring the viability of the U.S. defense industrial base and seeking to ensure that it is capable of satisfying U.S. national and homeland security needs.

1.7.4 State and Local Security Partners

State and local agencies are often first on the scene of a transportation security incident. It is the responsibility of Federal officials to work closely with regional preparedness organizations to coordinate recovery efforts and restore public confidence

following an attack. These agencies also work in close proximity to the owners or operators of the Nation's transportation infrastructure. Public safety agencies, such as law enforcement, fire/rescue, and emergency medical services (EMS) continue to be an integral part of gathering transportation security information and sharing it with the private sector owners and operators.

Additionally, the sector is working with the American Association of State Highway and Transportation Officials (AASHTO). AASHTO's Special Committee on Transportation Security (SCOTS) is responsible for advocating a secure transportation system by coordinating and collaborating with AASHTO members and other agencies and professional organizations. SCOTS membership includes three members (one voting member) from each member State. SCOTS has coordination interfaces with other AASHTO standing committees and subcommittees, such as the Standing Committees on Aviation, Highways, Public Transportation, Planning, Research, Rail Transportation, and Water, as well as subcommittees on Highways, Bridges and Structures, and Systems Operation and Management. In addition, AASHTO provides for security research through the Transportation Research Board (TRB) Cooperative Research Program.

1.7.5 Private Sector and Other Infrastructure Owners and Operators

Enhancing critical infrastructure security within the Transportation Systems Sector is a responsibility shared among all security partners—Federal, State, local, and tribal governments, as well as the private sector owners and operators. Since the private sector, as well as State and local entities, own and operate the majority of the transportation systems, a collaborative working partnership between the Federal Government and the private sector in fortifying all CI/KR security efforts and initiatives from their inception is essential. Therefore, the Federal Government must leverage industry's efforts in protecting critical assets through an effective public-private partnership. One manifestation of this partnership is mode-specific SCCs. A description of each modal SCC appears in its respective modal implementation plan annex.

1.7.6 International Organizations and Foreign Countries (International Activities)

The United States is an important trading partner with numerous foreign countries. Large volumes of merchandise enter the United States daily on ships and airplanes from across the world and by trucks and rail from multiple points along the Canadian and Mexican borders. However, the September 11, 2001, attacks highlighted the security vulnerabilities now inherent in the global transportation network. The Transportation Systems Sector recognizes the need to engage with international partners to: (1) identify and understand threats, assess vulnerabilities, and determine potential impacts to the global transportation system; (2) exchange and share effective practices to deter, understand, and prevent future attacks; and (3) promote measures that safeguard the movement of people, goods, and services through international transportation systems.

It is vitally important that our global partners share critical information. This partnership will lead to more informed decisions by identifying and understanding threats, vulnerabilities, and consequences using global threat information and assessments. The Transportation Systems Sector (TSA, GCC and SCC members, etc.) must work together in order to improve and enhance security while maintaining an efficient flow of goods between international trading partners. Examples of this cooperation are the Security and Prosperity Partnership of North America (SPP), which establishes ongoing working groups, including representatives from various Federal agencies and Canadian and Mexican ministries to further North American security goals, and the International Maritime Organization (IMO), a specialized agency of the United Nations, which is responsible for measures to improve the safety and security of international shipping and to prevent marine pollution from ships. TSA has taken a leadership role in coordinating such relationships. Asia-Pacific Economic Cooperation (APEC) is the premier forum for facilitating economic growth, cooperation, trade, and investment in the Asia-Pacific region, and TSA played a key role in launching the Aviation Security Sub-Group in APEC.

Many security enhancement efforts are already underway; however, the Transportation Systems Sector, through the leadership of TSA, has identified several key strategic focus areas. These areas are: (1) assisting the International Civil Aviation Organization (ICAO) in the area of compliance and enforcement to ensure that aviation security vulnerabilities are identified

through the Universal Security Audit Program; (2) increasing international focus on the need for pipeline, freight rail, and mass transit standards and/or best practices; (3) enhancing the ability of key international partners to identify terrorists and/or the instruments of terrorism by sharing technological expertise, lessons learned, and developing new advanced approaches; (4) strengthening international security baseline standards by actively participating in standard-setting organizations; (5) providing effective mechanisms for sharing and reporting information to foreign authorities and stakeholders through expert-level working groups, private conferences, bilateral meetings, and speeches; and (6) minimizing disruptions to the flow of passengers and commerce through regular consultations with international partners to discuss differences in policy or approach, working toward harmonization of measures.

Strengthening transportation security across all modes of the global transportation network requires strong collaboration worldwide to protect the traveling public from terrorism 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:

- The European Union (EU) (across all modes of transportation);
- European Civil Aviation Conference (ECAC);
- Asia-Pacific Economic Cooperation (across all modes);
- Civil aviation commissions in Latin America, Middle East, and Africa;
- The Group of 8 (the G8 is an international forum for the governments of Canada, France, Germany, Italy, Japan, Russia, the United Kingdom, and the United States) (across all modes);
- International Rail and Mass Transit Working Group;
- International Civil Aviation Organization;
- United Kingdom (Joint Contact Group, partnering at ICAO, and rail security);
- France (security cooperation and technical exchanges);
- Japan (technical exchanges and policy development, the 2006 Ministers of Transport Meeting in Tokyo, G8 coordination);
- Canada (pre-clearance, air cargo, Man-Portable Air Defense System (MANPADS), Smart Border, and SPP);
- Mexico (strengthening national-level oversight, MANPADS, ICAO audit preparation, and SPP); and
- Aruba, Bahamas, and Bermuda (aviation pre-clearance measures).

1.7.7 Other Advisory Councils

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. The committee will provide advice and recommendations to the administrator for improving aviation security measures.

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 stakeholders 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 in 2020. The Security Committee of the Council works closely with USCG, TSA, CBP, and other stakeholders to address issues of cargo, port, and container security.

National Infrastructure Advisory Council (NIAC). NIAC is the President's principal advisory panel on CIP 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 CI/KR areas as delineated in HSPD-7. 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 CIP, including DHHS, 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 will provide 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 security threats, international cooperation on security issues, and the security 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, and U.S. Army Forces Command—with responsibilities for 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 15 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 DOC's 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 agency with true metrology expertise (the only national metrology institute), has developed numerous homeland security-related minimum performance standards, participates (membership and committee chairmanships) in several standards setting bodies (American Society for Testing and Materials, National Fire Protection Association, International Association of Chiefs of Police, National Institute of Justice, Institute of Electrical and Electronics Engineers, Inc., etc.) 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. This is accomplished through the development of standards, metrics, tests, and validation programs, as well as establishing the minimum security requirements for Federal systems. NIST guidance aids 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.

1.7.8 Academia, Research Centers, and Think Tanks

National Research Council, Transportation Research Board (TRB). TRB is one of six major divisions of the National Research Council of the National Academies. The board 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 RDT&E in support of USCG's homeland security and non-homeland security missions.

National Laboratories and Technology Centers. DOE's laboratories and technology centers house world-class facilities where more than 30,000 scientists and engineers perform cutting-edge research. The 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.

Homeland Security Centers of Excellence. Through the Homeland Security Centers of Excellence (HS-Centers) program, the DHS is investing 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. The DHS's 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.

Multidisciplinary Center for Earthquake Engineering Research (MCEER). MCEER, headquartered at the University of Buffalo, comprises a consortium of researchers and industry partners from numerous disciplines and institutions throughout the United States. MCEER's mission has expanded from its original focus on earthquake engineering to one that addresses the technical and socio-economic impacts of a variety of hazards, both natural and manmade, on critical infrastructure, facilities, and society.

The John A. Volpe National Transportation Systems Center (Volpe Center). DOT's Volpe Center in Cambridge, Massachusetts, is an internationally recognized center of transportation and logistics expertise. The center assists Federal, State, and local governments, and industry and academia in a number of areas, including human factors research; system design, implementation, and assessment; global tracking, strategic investment, and resource allocation; environmental preservation; and organizational effectiveness.

Homeland Security Institute (HSI). HSI's mission is to assist the DHS Science and Technology Directorate (S&T) and the DHS Operating Elements in addressing important homeland security issues, particularly those requiring scientific, technical, and analytical expertise.

2. Identify Assets, Systems, Networks, and Functions

2.1 Defining Information Parameters

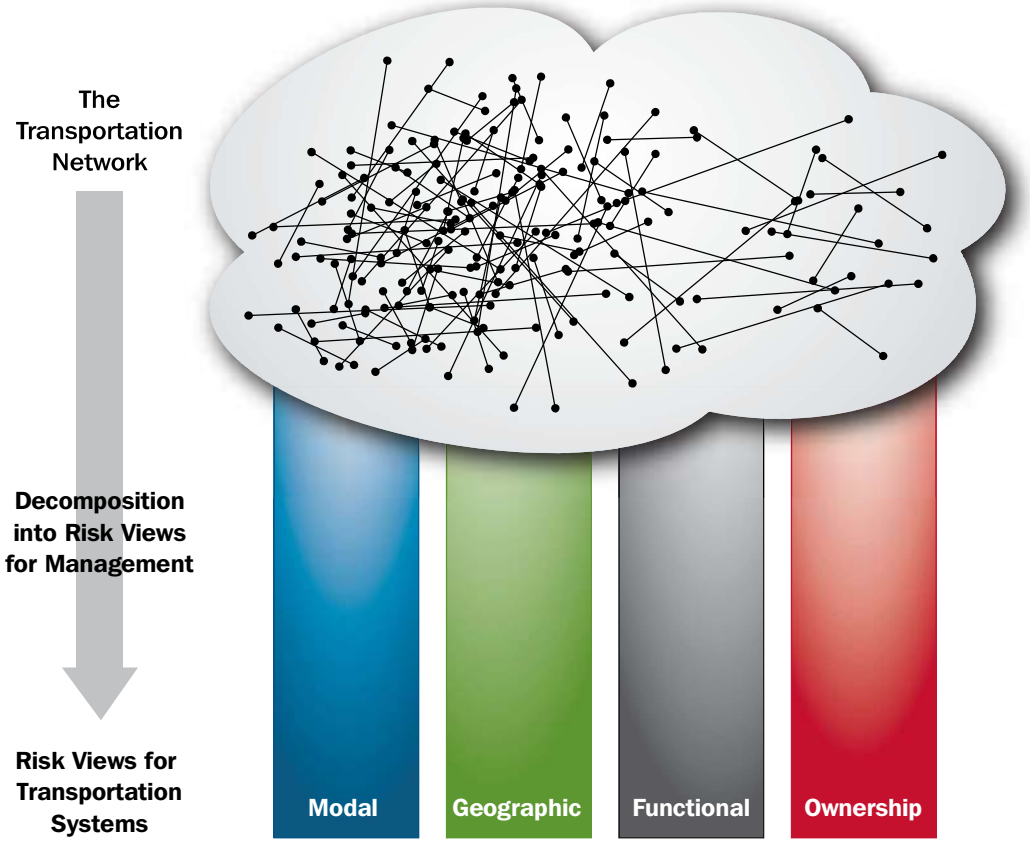
There are two complementary viewpoints from which the transportation network can be considered a system perspective or an asset perspective. A system is a collection of transportation assets, their relationships, and their emergent properties that collectively come together to perform a function, supported by institutional rules and regulations, and structured around processes. Assets include a node, link, or flow in a transportation system and can be physical, cyber, or human in nature. See the goals in section 1 for a more detailed definition. In this section, the asset-based approach to collecting infrastructure information will be expanded. A systems-based consideration of the sector will also be further detailed. The following sections detail the information parameters associated with both systems and assets and how that information is collected, verified, updated, and protected.

2.1.1 Information Parameters for Systems

The national transportation network is a large, multifaceted, interdependent mix of links, nodes, flows, processes, agreements, rules, relationships, and regulations. This complex cloud of activity must be reduced into more manageable data to be used for risk analysis.

To assist stakeholders within the Transportation Systems Sector in defining systems, thematic perspectives or risk views will be used. Risk views, illustrated in figure 2-1, are distinct and complementary ways of evaluating transportation infrastructure and defining transportation systems. They are not mutually exclusive, nor is it presumed that the data collected in these views will be collectively exhaustive. Instead, the risk view structure supports a scalable system analysis capability, allowing for the examination of how risk manifests in the system. Risk views are the first step in defining the boundaries of a system, establishing relationships within the system, and identifying interdependencies. The initial set of risk views includes:

Figure 2-1: Risk Views Within the Transportation Systems Sector



- **Modal:** Traditional industry delineation (i.e., Aviation, Maritime, Mass Transit, Highway, Freight Rail, Pipeline). All assets within a mode can be collectively evaluated as a system.
- **Geographic:** All assets within a geographic boundary (e.g., New York State or the city of Los Angeles). This view may be used most often by the G&T community, and State, local, and tribal government partners.
- **Functional:** All assets that, taken together, perform a specific function or service (e.g., supplying fuel to the Northeast). This view is supply chain-focused and may be used for example, by the USCG, CBP, interagency HAZMAT transportation working groups, and private sector partners.
- **Ownership:** All assets that fall under a defined set of decision rights, recognized by Federal, State, local, and tribal governments (e.g., all assets owned and operated by the New York Mass Transit Authority can be evaluated as a system).

2.1.2 Information Parameters for Assets

In working to protect the Nation's critical infrastructure, it is important that consistent terminology is used to facilitate communication and disseminate security information. Because the Transportation Systems Sector has a wide array of stakeholders, including commercial and industrial owner/operators and various Federal, State, and local agencies, it is important for the sector to adopt a taxonomy that will serve as the basis for how infrastructure is categorized within the National Asset Database (NADB).

The NADB is the Federal Government's repository for information on the evolving, comprehensive inventory of assets that comprise the Nation's infrastructure. The NADB taxonomy first groups CI/KR into the 17 broad sectors established in HSPD-7 and then categorizes them in more detail as needed. Up to five levels of detail are used, although not all infrastructure components require each level. Some infrastructure elements fall into more than one sector or have multiple components that fall into different categories of the taxonomy. In these cases, more than one sector or category is assigned to the piece of infrastructure. The SSAs (TSA and USCG), in addition to the DHS and DOT, have taken a comprehensive, integrated view of assets, including all characteristics and cross-sector CI/KR dependencies necessary for an asset to function. This integrated view is necessary because the functionalities of many assets depend on multiple elements and systems (e.g., people, electrical power, information technology (IT), or telecommunications). For the NADB transportation taxonomy, see appendix 5.

2.1.3 Information Parameters for Cyber Networks

The Transportation Systems Sector derives its understanding of critical cyber networks and assets from the USA PATRIOT Act; Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources; and HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection. The sector defines cyber networks as:

- An interconnected set of resources under the same direct management control (e.g., budgetary/operational authority for day-to-day operations and maintenance; system owners have the capability to effect changes in all areas that fall within the boundary of the system).
- An interconnected set of resources that have the same function or mission objective (entities within multiple systems that have identical/similar images and are geographically dispersed should be considered separate systems).
- An interconnected set of resources that have essentially the same characteristics and security needs (e.g., point of presence[144] defines a system; local area networks (LANs) and wide area networks (WANs) are different systems; persons under the Information System Security Officer (ISSO) manage security needs and administrative controls).
- A set of interconnected resources that reside in the same general operating environment (e.g., the ISSO must be able to see that operational controls are being enforced on day-to-day basis, attend to security incidents, and monitor/address security controls).

Collecting cyber data will be performed in the same manner as collecting data on physical transportation systems and assets.

2.2 Collecting Infrastructure Information

The collection of infrastructure information for the Transportation Systems Sector will cut across the four risk views (in addition to collecting asset-based data) to build a data set that is as comprehensive as possible. While this method may not be traditional in the way that owner/operators view their systems, it is reflective of the needs and responsibilities associated with the Federal perspective. One of the key advantages of constructing a data set from the four different perspectives on risk is that it builds a broad picture of the sector, which enables rich, system-based analyses. This also allows members of the sector to realize their place within the sector and understand how their system relates to others.

The ongoing effort to collect information will rely on data gathered from public and commercially available databases and from all Federal agencies and owner/operators who are requested to voluntarily submit CI/KR data on an as-needed basis. Existing statutory requirements can be a good source of infrastructure information; however, there are no standard collection requirements across the Transportation Systems Sector. Overall, the infrastructure identification process will continue to rely heavily on current processes and information sources. Where significant gaps exist, the sector will try to identify commercially available resources or request data from the owner/operator community. These data requests to the owner/operators will be

[144] A PoP (point of presence) is the location of an access point to the Internet.

voluntary, and those from the private sector will be encouraged to use the Protected Critical Infrastructure Information (PCII) Program when submitting information. The DHS is committed to protecting sensitive and confidential data from unintended disclosure using a variety of classification approaches in addition to PCII.

TSA is responsible for developing an understanding of data collection for asset dependencies, interdependencies, and critical functionality beyond what is required for the NADB, including collecting and storing system-level data. In conjunction with the GCC and the SCC members, the Transportation Systems Sector will work to identify targeted data sets, based on SROs, that are required to accomplish risk-informed security activities. While the NADB is currently asset-focused, the Transportation Systems Sector will seek to build a systems perspective into the existing NADB. This will not result in a secondary repository for information, but rather enhance the existing NADB.

In collecting cyber asset transportation data, TSA will use previous data collection efforts (e.g., the NADB); current TSA data collection approaches (e.g., Corporate Security Reviews, Risk Assessments, Rail Inspections, Commercial Site Vulnerability Checklist for Cyber Assets); and publicly available information, such as Securities and Exchange Commission filings. The GCC/SCC construct will serve as the primary vehicle for sharing cyber asset data within the sector. Cyber asset information will also be shared on an as-needed basis with other sector lead agencies, such as the National Cyber Security Division (NCSD) (Communications Sector) and the DOE.

Data gathered will be used in a variety of ways throughout the risk assessment and prioritization processes. Uses of the information will include, but are not limited to, risk assessments on systems, interdependency analyses, infrastructure modeling, infrastructure prioritization, and reporting. The Transportation Systems Sector will ensure that information protection mechanisms are in place to protect against misuse, unauthorized disclosure, or theft.

2.2.1 Data Collection Efforts: Systems

Collecting data through the systems risk view focuses on multiple, heterogeneous, geographically distributed systems that are embedded in networks at multiple levels. The four views capture multiple ways of addressing systems and add to a more robust assessment of the sector.

Modal View. The modal view treats all classes of assets within a mode collectively as a system. Infrastructure information in the modal view is categorized by interdependencies and supply chain implications that are specific to a particular mode of transportation. In addition to focusing on individual assets, nodes, and links, information specific to the modal view includes how those assets, nodes, and links interact within the mode and with other modes, their emergent properties and governing principles, or legislative information with specific modal impact. The sector will collect data through existing mode-specific data lists and readily available databases. Sector partners, in cooperation with other Federal agencies, State and local governments, the GCC and SCC, trade associations, nongovernmental organizations, and industry subject matter experts, will work to build a complete data set to best understand the risks to these modes.

Geographic View. The geographic risk view compiles transportation infrastructure data within specific regions of the Nation. The boundaries of those regions may vary based on the purpose and necessary parameters of an assessment. Regions may contain markedly different assets and systems, and thus the risks to those systems and the types of data collected from those regions will differ as well. Data collection in this view will allow an information set to be defined by what is physically located within that region and the processes or policies that impact that specific region. Therefore, assets, links, nodes, and emergent properties within a defined geographic area are evaluated as an integrated system.

Functional View. The functional view of data collection looks at the function a system fulfills within the supply chain. Examples of a functional view of systems include all of the assets, links, nodes, processes, policies, and emergent properties associated with:

- Delivery of critical medicines;

- Delivery of chlorine for drinking water or other purposes; and
- Delivery of heating oil to the Northeast.

By examining the function a system plays in society, the critical aspects of the system can be measured. This view also will have value in identifying interdependencies with other critical infrastructure. Collection efforts in the functional view are in the early stages and will be expanded over time.

Ownership View. The private sector owns approximately 85 percent of the Nation's assets. The ownership view examines information on ownership of assets, including the owner/operator's decision structure, policies, and procedures, and recognizes those assets owned by the same entity as an integrated system. Any data requested from owner/operators by the Federal Government for risk analysis need not be all-encompassing. Rather, infrastructure information required from owners by the Federal Government will be targeted and based on SROs.

2.2.2 Data Collection Efforts: Assets

Asset data is segmented by the six transportation modes. Data collection efforts by the Transportation Systems Sector will not attempt to be all-encompassing. In addition to using asset data collected in the NADB, the sector security partners will establish SROs through the SBRM approach, and only targeted data related to those SROs will need to be collected. The Transportation Systems Sector plans to employ the GCC/SCC framework to aid in the process of identifying and acquiring that targeted asset data. Specific information concerning the data collection efforts of individual modes can be found in the respective modal implementation plan annexes.

2.3 Verifying Infrastructure Information

Because of the complexity and size of the sector, sufficient resources do not exist to verify asset and system data for the entire sector. The Transportation Systems Sector will rely on stakeholders, including leading industry organizations and Federal, State, and local agencies, to help verify input. Federal infrastructure information compiled by other Federal agencies and used by the Transportation Systems Sector will be accepted as complete and not require immediate verification. For all risk views, multiple sources of information will allow cross-confirmation and the maintenance of a complete and up-to-date data set. Currently, a single methodology for verifying cyber asset information received from sector members outside of TSA has not been identified or employed. The SSAs will review currently available asset-specific information and group assets based on functionality and mode.

2.4 Updating Infrastructure Information

The SSAs intend to work with the DHS IP to expand the method for capturing systems information. Once asset and system information is verified, the sector will rely on sector stakeholders, including leading industry organizations and Federal, State, and local agencies, to help update and validate important infrastructure data. To improve stakeholder communications and expedite the flow of asset information, the Transportation Systems Sector will work across GCCs, SCCs, and Information Sharing and Analysis Centers (ISACs) to coordinate information updates.

2.5 Protecting Infrastructure Information

Information used and needed by the DHS and its security partners to effectively manage risk and secure the Nation's critical infrastructure often contains security information and/or sensitive business and proprietary information. As a result, information protection is paramount for those security partners who voluntarily supply critical information. The DHS has tools to protect security information by using the PCII Program. The program is managed by the DHS PCII Program Office within the

Partnerships and Outreach Division (POD). The PCII program will protect proprietary and threat information from the private sector. The PCII Program will be administered by the National Infrastructure Coordination Center (NICC). The rules governing the PCII Program are located in Title 6, Part 29 of the Code of Federal Regulations (CFR). General information on the PCII Program is found on DHS's Web site at www.dhs.gov/pcii and in the NIPP base plan.[145]

Other regulations, in addition to the PCII Program, may affect the protection of data submitted to the DHS. For example, DOT and the DHS have regulations for protecting Sensitive Security Information (SSI) (49 CFR Parts 15 and 1520). Information is protected as SSI if it meets the definition of any of the specific categories of SSI established in parts 15 and 1520, or if it otherwise must be protected from disclosure in order to ensure transportation security. Similarly, 46 United States Code (U.S.C.) 70103(d) (as implemented by 49 CFR Part 1520) requires that maritime security information, especially security assessments and plans, be protected from unauthorized access or disclosure.

In addition to designating certain sector information as PCII or SSI, as appropriate, the Transportation Systems Sector must adhere to internal standards for protecting electronic information from a cyber attack. In a broad sense, TSA's compliance and oversight of the cyber security function is driven by goals set forth by legislation, regulations, policies, directives, and standards. In addition to OMB and the Federal Information Security Management Act (FISMA), the National Institute of Standards and Technology (NIST) was directed to produce numerous security documents. Because securing vulnerability assessment data is a central portion of the sector plan, TSA will use an integrated method to incorporate new security guidelines as they become available.

More information on the government's efforts to standardize and emphasize cyber security for all government facilities can be found in the Government Facilities SSP.

[145] For more information, visit www.dhs.gov/dhspublic/display?theme=92 or www.dhs.gov/dhspublic/display?content=5476.

3. Assess Risks

3.1 Background

The Transportation Systems Sector faces a dynamic landscape of potential natural disasters, accidents, and terrorist attacks. To address the challenges posed by such risk, the sector will employ a comprehensive risk management program. Improving the overall risk profile of the sector will require an integrated asset- and system-based risk management approach. Asset-based risk management, essential to sector security, is widely practiced. However, transportation risk is not usually mitigated by "point" solutions alone (e.g., improving airport screening or erecting fences around a train station). Therefore, the sector will integrate asset-based risk management with a strong systems analysis designed to address the complexity of the transportation network. A systems perspective is needed to account for network vulnerabilities and potential ripple effects—conditions created because of the interconnectedness and interdependence of transportation assets, systems, and functions nationwide. Such a focus facilitates informed prioritization of decision options for securing critical assets, laying the foundation for a more effective and informed implementation of traditional asset-based approaches. The Transportation Systems Sector SBRM approach will identify and manage the sector's risk profile; develop standards and criteria for a common, relevant operational picture; and generate a portfolio of alternative management strategies that sector leaders can use to improve action and investment agendas.

Consistent with Secretary of Homeland Security Michael Chertoff's vision for risk management, the Transportation Systems Sector's approach recognizes the important role that threat, vulnerability, and consequence play in the overall risk profile. Because of the difficulty in predicting terrorist threats, as well as the myriad vulnerabilities that exist in the transportation network, the sector is adopting a view of risk primarily driven by consequence. SROs will flow from an understanding of high-consequence risks to the network and will enable sector leaders to manage risk appropriately and effectively. Materiality, a blend of consequence and likelihood, will help to identify and prioritize SROs.

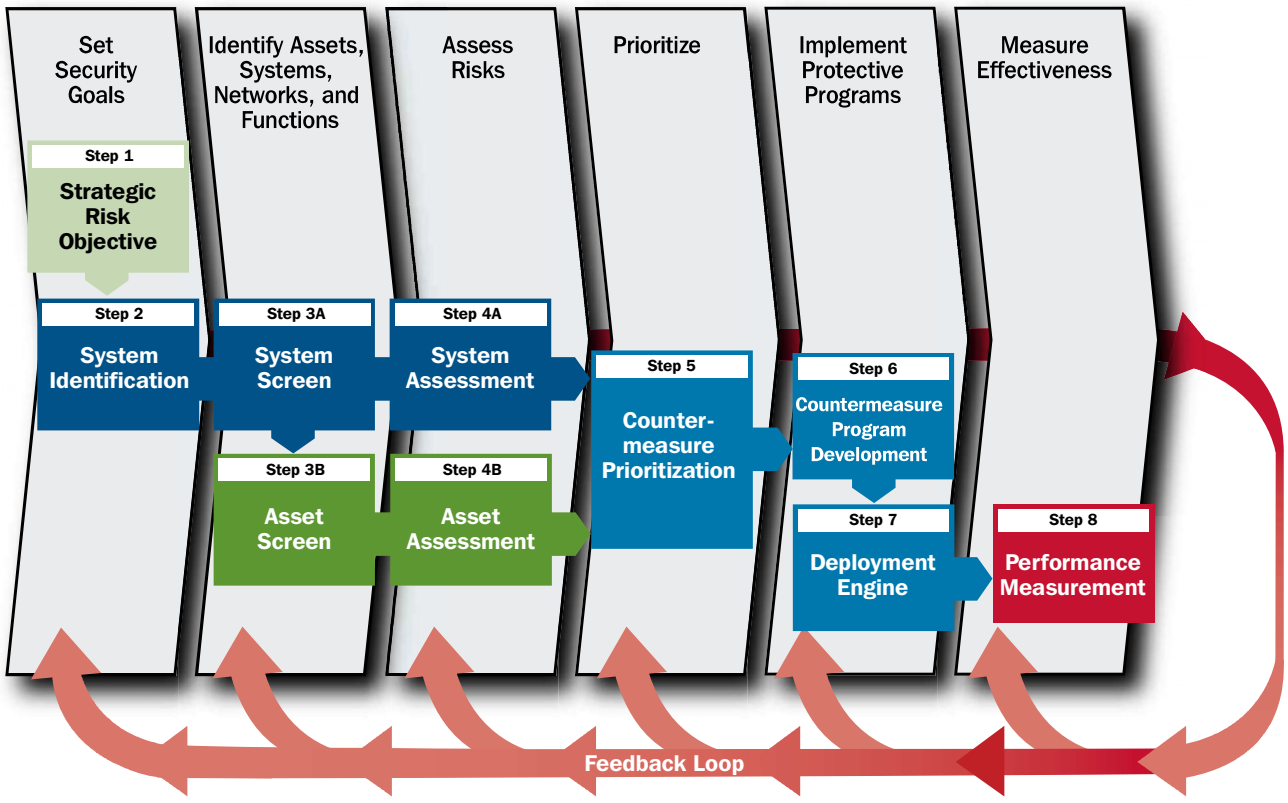
The approach described in this SSP is not the beginning of risk assessment for the sector, which has been ongoing for years and is crucial to transportation security; rather, it builds on existing programs to deliver an integrated systems-based approach. The SSAs will be responsible for coordinating this effort across the sector. Of course, risk management throughout the sector will be done in partnership with State, local, and tribal governments and with private sector owners and operators. Owners and operators assess their own assets and manage the risk to those assets, in some cases with assistance in various forms from the Federal Government. Information gathered through assessments and analyses enables the sector to consider which combination of countermeasures for assets, networks, systems, and functions will require risk management action and how those should be best applied at both the asset level and the systems level.

3.1.1 Relationship to the NIPP Guidance

To ensure the overall effectiveness of the Transportation Systems Sector's risk assessment methodology, the general approach described in the NIPP and the SSP guidance has been translated into a multi-step process—the SBRM methodology—that drives

the development of mitigation options (e.g., risk management/countermeasure options). Each element of the NIPP guidance is addressed in the methodology, as shown in figure 3-1 below. While there are differences in terminology, the individual components of the SBRM approach directly relate to the objective of the NIPP risk management framework.

Figure 3-1: NIPP Risk Management Framework/Systems-Based Risk Management Process



3.2 Overview of the Transportation Systems Sector SBRM Methodology

The complexity and magnitude of the transportation network requires a robust and continuously informed risk management process. The SBRM methodology allows for sector-wide identification of and planning for those risks that, if realized, would have the most serious consequences for the transportation network. SBRM does not take the place of existing asset-based protection, nor is it intended as an operational or tactical plan. Instead, it takes a broader perspective and shifts the focus of the sector from specific point solutions to system-wide risk management. These perspective shifts are explained below.

3.2.1 Shifting From ASSETS to SYSTEMS

Asset-based data collection and risk assessment are underway across the sector and are an important component of transportation security. In the maritime mode, for example, the USCG's maritime security regulations at 33 CFR subchapter H that require facility and vessel security plans have generated information on thousands of maritime assets. The USCG continually reviews this information in its risk analysis. A systems-based approach examines how assets and systems interact with each other and the negative effects one could have on another if disrupted.

3.2.2 Shifting From REACTIVE to ADAPTIVE

Given increasing complexity and a constantly evolving threat environment, Transportation Systems Sector risk management must also be capable of adjustment and response to changing conditions. Flexible security measures and improved information sharing greatly enhance the sector's ability to respond to changing threats.

3.2.3 Shifting From EVENTS to PATTERNS

Although a major consequence is a concern, it is the repetitive occurrence of terrorist attacks worldwide that will show patterns and, in recognizing those patterns, security measures can be identified.

3.2.4 Shifting From RIGID to RESILIENT

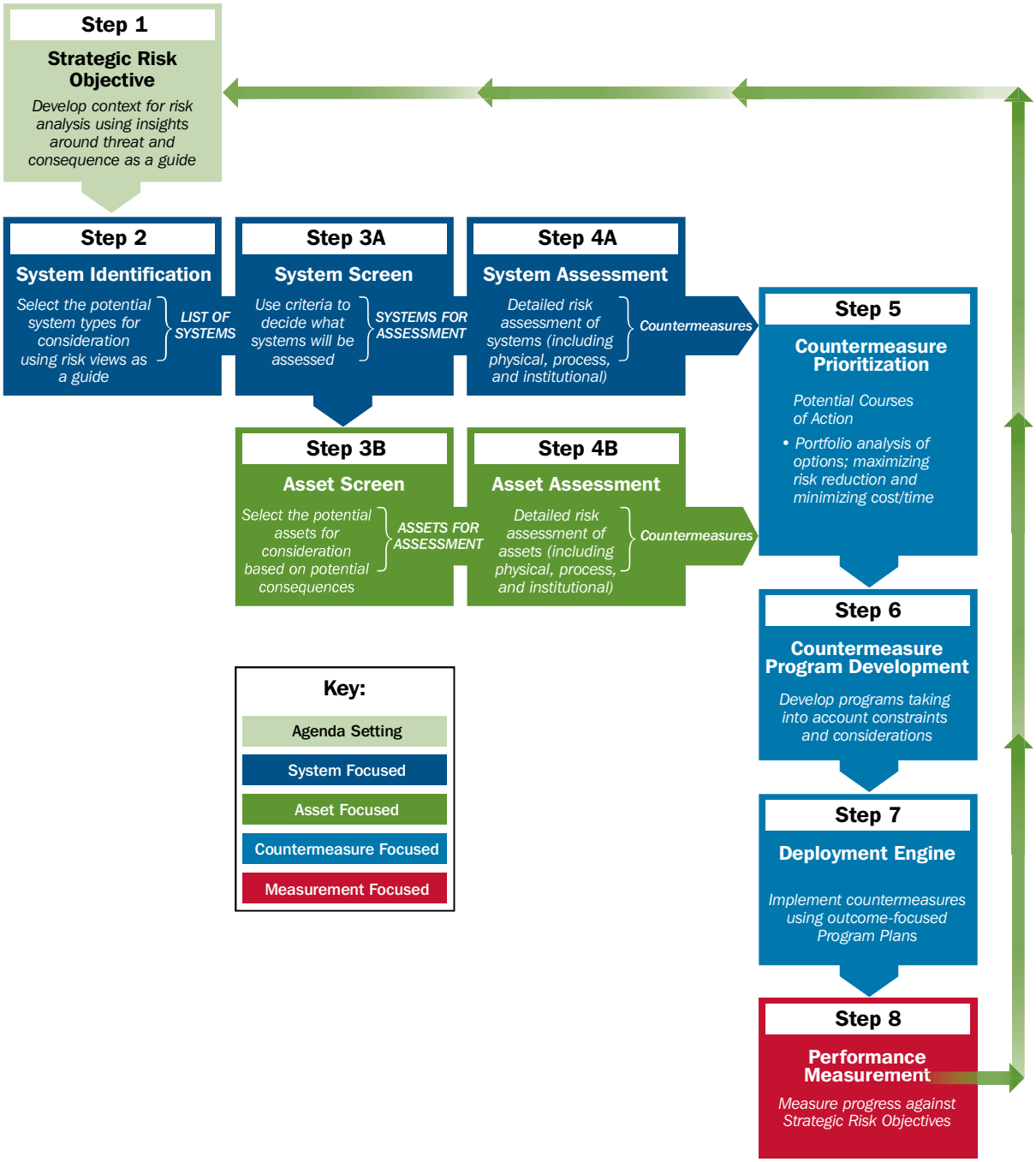
"Hardening" is an essential component of protecting critical assets and infrastructure. However, resilience of the transportation system can be improved by increasing its ability to accommodate and absorb unexpected shocks from natural disasters or terrorist attacks without catastrophic failure. Resilience-improving strategies include a wide variety of mitigation activities, including response and recovery activities.

The shifts in perspective allow the Transportation Systems Sector to view risk more accurately. By examining systems along with assets and focusing risk mitigation options on SROs likely to have the greatest impact on the network, resources can be more effectively allocated.

There are innumerable risks to the transportation network and an innumerable set of risk mitigation options. To meet the goal of continuously improving the risk profile of the transportation network with reasonable costs, the sector's varying stakeholders must focus and coordinate their respective efforts. To achieve such coordination, there must be focused and direct statements of intent from sector leadership. SBRM defines these statements as SROs. As previously stated, SROs, developed by both public and private industry leaders, are statements that establish a specific, measurable, realistic, attainable target that, when achieved, will improve the sector's risk profile. SROs are the driving force behind all risk-related decisions for the transportation network.

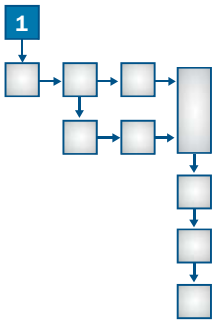
With clearly stated SROs as the planning guidance, the sector, as a whole, is able to identify systems and assets that require detailed risk assessments, prioritize countermeasure packages, develop countermeasure programs, implement effective programs, and monitor progress against objectives. As the methodology is inclusive of current ideas and tools, much of the ongoing risk-related activities performed by stakeholders fit within this framework. The following sections describe the steps of SBRM in detail, and figure 3-2 is highlighted to emphasize each step.

Figure 3-2: Systems-Based Risk Management Process[146]



[146] As SSAs, TSA and USCG, in collaboration with DOT, are the leads for implementation of the SBRM process in cooperation with government and private sector partners.

3.3 SBRM Step 1: Setting the Strategic Risk Objective



In order to make the process of risk management both tenable and effective, the GCC and SCC must focus on a specific set of objectives. As an initial step to establishing SROs, leaders from across the sector, specifically including private industry, will meet to discuss priority strategic risks. The intent of setting SROs is to enhance the current set of sector goals and objectives. Those SROs will be based on the materiality of certain consequences and the inability of the owner/operator community to address the priority risk without some form of Federal assistance. Full cooperation from the leaders of the sector, both public and private industry, is essential to establishing appropriate, realistic SROs. With consensus and cooperative efforts, the SROs will move from statements of intent to the motivating factors uniting sector-wide risk management efforts.

A defining characteristic of the sector's mission is that it is an ongoing activity—*continuously improving the risk posture of the national transportation system*—so the SROs cannot be static. Stated another way, an ongoing mission, like that of the Transportation Systems Sector, needs a constant stream of objectives inserted to ensure that the evaluation process is continuously utilized. The compilation of these objectives sets the direction for the management of strategic risk within the transportation system.

As discussed in section 1, each outcome-focused, sector-specific SRO developed will be supported by security measures designed to make measurable progress against the mission. Cross-cutting strategic goals will provide a framework to ensure that the sector deploys a balanced, comprehensive set of security measures to accomplish its SROs. In short, the SRO helps to clarify "what to focus on" based on the best available information. The strategic goals clarify "how to focus" based on public and private sector national priorities and lessons learned.

Once SROs have been identified, countermeasure programs that address those objectives will be coordinated within and across the security partners that compose the Transportation Systems Sector. In the interim, strategic goals outlined in section 1 have been developed to ensure progress against the mission.

The key to identifying a potential SRO is to capture it as an objective rather than a large-scale threat scenario. Table 3-1 shows the difference between the two concepts.

Table 3-1: Strategic Risk Objectives Compared to Threat Scenarios (Examples)

Strategic Risk Objective	Large-Scale Threat Scenario
Minimize the likelihood and impact of an attack on a major U.S. transit system.	Coordinated subway bombings
Prevent the destruction of U.S. aircraft by terrorists.	Improvised explosive device (IED) detonation during a flight
Minimize the likelihood and impact of an attack on a key, multi-modal transportation hub to the regional transportation system and to the national economy.	Release of bio-agent in a large airport
Minimize the likelihood and impact of an attack on an in-transit HAZMAT shipment on the U.S. transportation system.	Detonation of HAZMAT truck in a densely populated area
Minimize the likelihood and impact of a significant tunnel breach to the regional transportation system and to the national economy.	Tunnel breach and subsequent flooding of a city

3.3.1 Strategic Risk Objective Inputs

The process for determining SROs will be informed from three main sources: the intelligence community, expert judgment, and futures analysis. Each group will provide inputs based on its unique point of view. For example, the intelligence community may produce a fact-based review of current (classified) analyses to determine the most likely risks to the transportation network. The transportation industry professional community, including government and private sector stakeholders, will provide insight on the most likely risks to the system based on the intimate knowledge of existing transportation operations and the current security landscape. The futures analysis[147] group may use Red Cell or Alternative Futures review of current analyses to assemble and describe the most likely risks to the national transportation system based on their expertise. Each group's unique perspective is essential to formulating relevant and effective SROs.

Figure 3-3: Inputs for Strategic Risk Objectives

3.3.2 Consequence-Driven Strategic Risk Objectives

The SRO formulation process is grounded in an understanding of consequence. The sector's consequence assessment methodology considers a variety of factors, as discussed in the NIPP. The interconnected nature of sector risk is also key to determining consequence. Emphasizing consequence captures the difficulty associated with predicting terrorist threats; it also focuses on the overall effect of an attack—the potential human, economic, and psychological losses associated with terrorism. The following sets of questions exemplify consequence-based thinking:

- **Health and Human Safety.** What is the impact of a particular scenario on human life and physical well-being? For example, what levels of fatalities can be expected—either early or latent (e.g., as a result of diseases contracted or injuries sustained)?
- **Economy.** What is the impact of a particular scenario on national, State, and local economies? What are the expected costs of response and recovery? What is the expected cost of rebuilding assets or systems? To what extent will business operations and/or supply chains be disrupted and for how long?

[147] Futures analysis is a process in which an enterprise conducts long-term insightful research and analysis to better understand potential environment changes and identify the enduring strategies and capabilities necessary to achieve its mission in the future.

- **Mission.** What is the impact of a particular scenario on the Federal Government's ability to maintain order, deliver essential public services, ensure public health and safety, and carry out national security-related missions?
- **Public Confidence.** What is the impact of a particular scenario on public morale and confidence in national economic and political institutions? If public confidence were to suffer, what would be the associated impacts on governance and the economy?

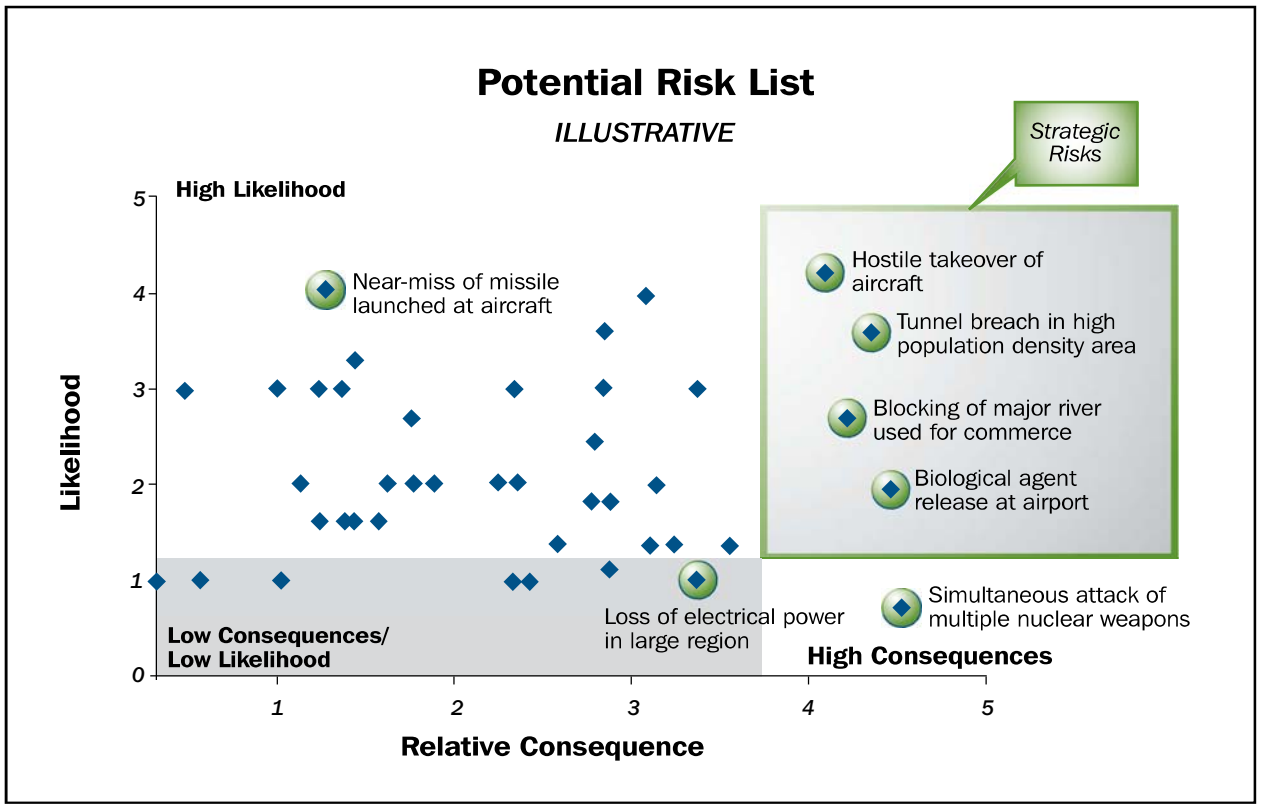
3.3.3 Materiality of Threats

For the sector's purposes, materiality is a function of likelihood and consequence for a given event. A threat is *material* if its manifestation could negatively and substantively affect the health and safety of the citizens, the national economy, the environment, public confidence, or the ability to conduct the business of governance.

An essential element of the consequence-driven risk management approach is the ability to address the escalating scale of consequence that comes about as a result of the "network effect." The term "network effect" refers to the exponential nature of systems, where every additional user increases the likelihood of even more users. Materiality depends on both the relative size of the impact and its likelihood of occurring. Since formulating SROs is fundamentally an expert judgment-driven process supported by information from the intelligence community, materiality provides a threshold or cut-off point to help defend and explain the selection of a given risk objective.

Figure 3-4 demonstrates how materiality can be used as a means of structuring the potential threats facing the transportation system. Each dot on the chart represents the combined likelihood and consequence of a threat.

Figure 3-4: Materiality Mapping of Potential Threats to the Transportation System



In the above figure, threats with a high relative consequence ranking and a high likelihood of occurrence represent greater materiality than those in the low/low quadrant. However, the other two quadrants still represent critical areas for consideration when assessing risk within a system. Each of the other quadrants has a "high" ranking in either consequence or likelihood, which means that each will be given consideration against the decision criteria.

Since the determination of materiality is a qualitative process, a variety of techniques will be used to extract the critical insights necessary to make this process transparent, traceable, and defensible. All these techniques will draw upon a wide array of technical and policy experts from across government, business, and academia in focused panels, interviews, and analytic sessions.

3.3.4 Assessing Threats

General Threat Environment. SROs will be formulated with a keen awareness of the various threats facing the sector. The chief threat is from terrorism. As the Brookings Institution noted, "from 1991 to 2001, 42 percent of all terrorist attacks worldwide have targeted rail systems or buses."[148] Terrorists understand that the open nature of the Transportation Systems Sector's infrastructure and operations is essential to the economic well-being of major cities or regions and numerous industries. However, terrorist attacks are only one of a number of potential threats that the sector faces. Natural disasters, as witnessed by the catastrophic Hurricane Katrina, and industrial accidents, such as the large HAZMAT spill on I-95 in Connecticut, also have serious economic, political, and psychological impacts on the sector.

To assist in creating an understanding of the general threat environment, the DHS, in coordination with the National Counterterrorism Center (NCTC) and the intelligence community, is preparing general threat environment documents for each sector. The documents, called Strategic Sector Assessments, can be used by industry, State, local, and tribal entities to assist in determining risk. Assessments will be prepared for each mode (Aviation, Maritime, Mass Transit, Highway, Freight Rail, and Pipeline).

While stakeholders have a legitimate need for current threat information to take immediate defensive action when appropriate, in the context of the sector's risk management approach, strategic threat analysis will be used to inform SROs.

Cyber Threats. Cyber threats to the Nation's critical infrastructure are addressed in unclassified documents such as the *National Strategy to Secure Cyberspace*, as well as classified reports. The cyber threat requires a substantial commitment from the public and private sectors to properly align resources, assess vulnerabilities, and protect critical networks from attack. America's critical infrastructure is under constant cyber attack; however, these attacks are varied and usually reflect criminal behavior rather than terrorism. The Transportation Systems Sector will work with the NCSD and affiliated analysts and experts in the intelligence community to monitor, assess, and respond accordingly to threats against the sector.

Process for Threat Analysis. Numerous intelligence agencies, such as NCTC, have specific roles in providing threat information to the sector. NCTC provides transportation security intelligence information to the Office of Intelligence (OI) within TSA to produce classified and non-classified annual threat assessments by mode and for the cargo/supply chain sector since 2004. These reports are disseminated throughout TSA, the DHS, and private industry. To produce accurate and comparable risk assessments, the formulation of assessments must be understandable, thorough, and repeatable. The sector recognizes the importance of private industry integration into the full intelligence cycle, consisting of private industry's intelligence requirements, tasking, analysis, and dissemination.

While the intelligence community provides numerous streams of raw intelligence to the DHS, USCG, and TSA, this information must be analyzed, filtered, and disseminated to sector stakeholders as classification and threat levels warrant. These communications are intended to solicit immediate action by stakeholders, especially private sector operation and tactical efforts. Modal GCCs and SCCs must work together to engage subject matter experts at the Surface Transportation ISAC, Public Transit

[148] Arnold M. Howitt and Jonathan Makler, On the Ground: Protecting America's Roads and Transit Against Terrorism, The Brookings Institution Series on Transportation Reform, April 2005; see http://apps49.brookings.edu/dybdocroot/metro/pubs/20050426_howitt.pdf.

ISAC, Highway ISAC, Maritime ISAC, ISAC Council, Association of American Railroads (AAR) Operations Center, and other information-sharing bodies to ensure the proper dissemination of intelligence. The sector will consider establishing a joint intelligence working group to better coordinate further integration. For long-term planning purposes, analyses will be packaged in a format and clearance level that enables sector stakeholders to understand threat in the context of a broader systems perspective, thereby facilitating input for developing SROs.

The roles and responsibilities of the various stakeholders in the threat analysis process are described below:

- **Transportation Security Administration, Office of Intelligence (OI):** OI provides a capability to review, synthesize, and analyze transportation-specific intelligence. It is the only Federal entity focused solely on the security of the sector. OI intelligence products assist these critical TSA components in assessing risk and developing appropriate security programs, countermeasures, mitigation strategies, and protection guidance. The following is a list of the major OI threat assessment products (based on information received from NCTC and the intelligence community) that contribute to the sector's understanding of the terrorist threat:
  - Transportation Intelligence Gazette: Concise written assessment of transportation-related intelligence, threats, and incidents. Produced frequently, as warranted, by intelligence reporting.
  - Threat Assessments: In-depth written assessments of transportation-related intelligence and threat information.
  - Modal Threat Assessments: Comprehensive threat assessments, produced annually at the classified and For Official Use Only (FOUO)/SSI levels, of the terrorist threat to each of the major transportation modes (Aviation, Maritime, Mass Transit, Highway, Freight Rail, and Pipeline) and to the cargo/supply chain sector.
  - Special Threat Assessments: Written threat assessments of the transportation security implications of special events or dates of national significance (e.g., the State of the Union Address, the Super Bowl, and Independence Day) or international significance (e.g., the Olympics).
  - Weekly Field Intelligence Report: Weekly compilation and analysis at the FOUO/SSI level of terrorist threats, trends, incidents, and suspicious events that are pertinent to transportation security personnel in the field. Based on intelligence, law enforcement, and open-source reporting.
  - Suspicious Incidents Report: Weekly compilation and threat/statistical analysis of intelligence, law enforcement, and open-source reporting on transportation-related suspicious incidents.
  - Intelligence Notes: Classified and FOUO/SSI assessments of transportation-related threat information; terrorist trends; terrorist incidents; and terrorist tactics, techniques, and procedures.
  - Transportation Situational Awareness Notes: Written analysis/report of noteworthy transportation-related terrorist information, including threats; actual or attempted attacks; suspicious incidents; and tactics, techniques, and procedures.
- **United States Coast Guard, Intelligence Coordination Center (ICC):** ICC provides all-source, tailored, and integrated intelligence and intelligence services to the DHS and its component agencies, such as TSA, the USCG Commandant and staff, the intelligence community, combatant commanders, and other services and agencies.
- **Homeland Infrastructure Threat and Risk Analysis Center (HITRAC):** HITRAC assesses intelligence information at a strategic level, looking not at individual targets, but at the transportation network on a larger scale. Modal analysts liaise with TSA analysts to produce coordinated intelligence analytic products. Transportation subject matter experts from various other agencies are also made available to HITRAC as requested.

3.3.5 Cross-Sector Information Sharing

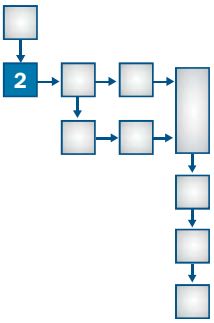
In the course of assessing and understanding threats to transportation infrastructure, communication among the sector stakeholders is vital to the overall security of the various systems. Many initiatives are already underway (discussed in section 8) and the sector will continue to support them.

As more risk data and analysis are available, ISACs and State and Local Fusion Centers (SLFCs) will become key players, helping to ensure that the necessary officials in the State, local, and tribal governments and the private sector are aware of their threat environment. TSA has piloted the deployment of Field Intelligence Officers to seven airports to directly support Federal Security Directors in their security duties, as well as build relationships with State and local stakeholders in the other modes.

DHS, TSA, and USCG analysts will continue to collaborate on numerous analytic products on threats to the sector and will work to disseminate assessments at the appropriate classifications to empower the greatest number of stakeholders with accurate and timely information. The Transportation Systems Sector GCC and modal GCCs will play central parts in building relationships with the sector stakeholders and in growing the trusted two-way exchange of information between private sector stakeholders and government risk management offices and leaders. This information-sharing effort is essential to meeting the priorities of the NIPP and the Transportation Systems SSP.

A feedback loop will also be established to ensure that insights gleaned from field assessments using specific threat input are shared with intelligence analysts throughout the intelligence community to continue to evolve their thinking and analysis. While State, local, tribal, and private sector needs for current threat information may still remain high, for the purposes of risk assessments, strategic threat objectives will be more applicable and useful to the sector in understanding its overall risk profile.

3.4 SBRM Step 2: System Identification

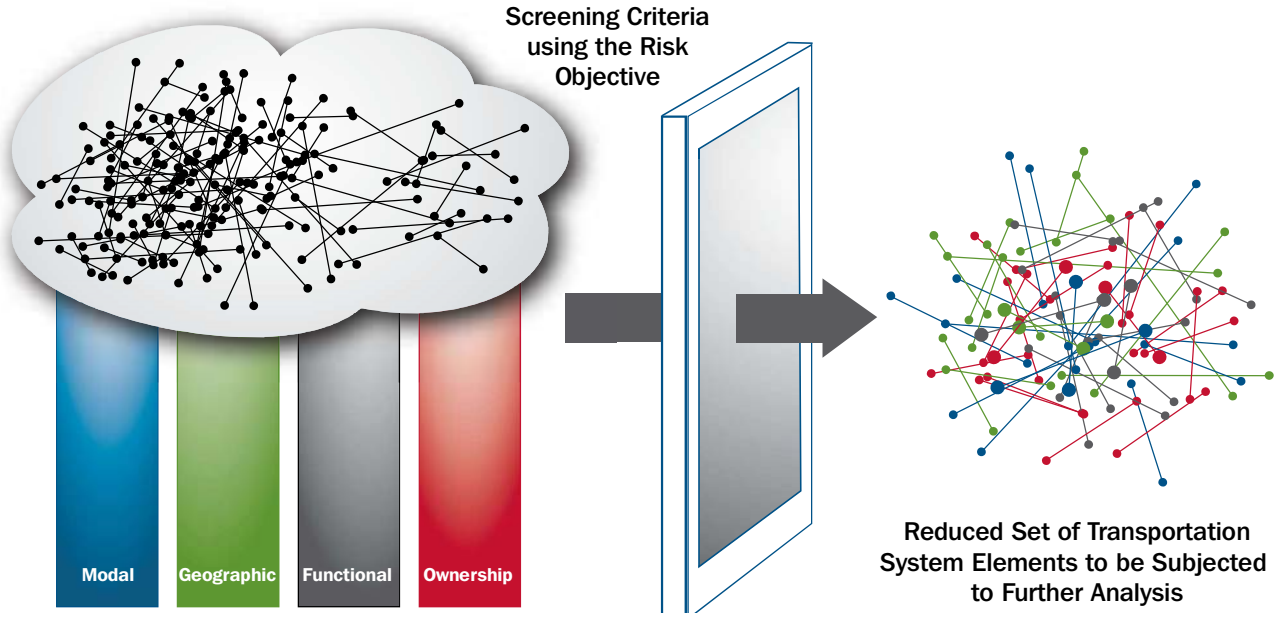


After an SRO is determined, the next step provides a formal review of the transportation network so that a feasible model can be developed and analyzed effectively. This step effectively reduces the "universe of options" by determining those transportation systems that have little to no impact on an SRO. For a risk objective such as "minimizing the downtime of large airports affected by a natural disaster," there may be a clear set of systems that need not be considered (e.g., rail, maritime) because they are effectively outside the scope of the analysis. Other objectives, such as "improve the ability of the transportation system to withstand the impact of a Category IV or V hurricane," will be more inclusive of modes and less inclusive of locations (geography). While an obvious initial step, identifying systems is crucial to the subsequent steps involving complex system and asset assessments.

3.4.1 Initial System Screening

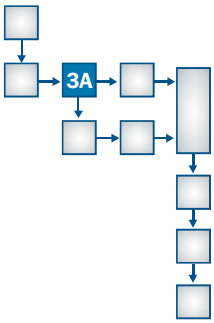
By using the different risk views—modal, geographic, functional, and ownership—as a guide, a more comprehensive list of systems will be generated. Effectively, this step reduces the universe of options by making a value judgment on transportation systems that have very little to do with a given objective. Figure 3-5 depicts the identification and filtering process.

Figure 3-5: Identification and Screening Process



Following the application of each view to the transportation network, the resulting system is further characterized. The SBRM output for this step is a reduced set of systems of potential interest to be considered in the system screening process that is defensible and traceable.

3.5 SBRM Step 3A: System Screen



Following step 2, a refined view of the system is ready for analysis. Step 3A allows for further refinement of the system to be analyzed and develops a working model that can be used to simulate scenarios pertinent to the SRO. These activities are achieved in three primary substeps:

- Apply system screen;
- Define system operations; and
- Baseline system performance.

3.5.1 Apply System Screen

Even the reduced set of systems from step 2 is challenging to evaluate and draw any meaningful conclusion from in a reasonable timeframe. Step 3A further filters the systems of potential interest using operational performance goals (baseline requirements for system operation derived from the SRO) as the basis to determine which subsystems and elements will be subjected to a much more detailed analysis. This step is analytically necessary given the often inverse relationship of system size to the specificity of the countermeasure. The SBRM framework strives to capture the most specific and action-oriented countermeasures possible. To do this, analysts need to be working with as reasonably sized and issue-focused a system as possible. Step 3A takes the systems determined to have a strong association with the SRO and selects from that set a reasonably sized and issue-focused system, and then baselines its performance for further study.

3.5.2 Define Systems Operations

Upon further filtering of the transportation network, defined in step 2, relationships and connections within the network need to be modeled and understood. To achieve this, a suite of network modeling tools can be used. A key output of this step is that an accurate rendering of the system under study has been captured and stored.

Network Structure of Each System. Relationships within the transportation network need to be defined at two levels. The first is to understand key interdependencies and linkages between assets. This leads to a representation of the various parts of the system as a network, where nodes are represented as assets and links represent the physical connections between these assets or nodes. Physical information about the transportation system can be acquired through relevant industry data sets and through experts in this realm.

Additional layers of information also need to be captured regarding the institutions and processes governing the system. To properly capture this information, experts may need to be solicited again. While information on institutional processes and procedures may be harder to capture, unlike the physical system, the key relationships between the three layers need to be understood and documented prior to moving to the next substep. However, it is also important to note that a complete data set is not required to move into the next step of the process.

Intersystem Relationships. The previous substep defines, characterizes, and illustrates different components of the transportation network. Additional research is also needed to document the relationships between these various systems. Key relationships exist between separate transportation systems. For example, the rail and aviation systems share common assets (e.g., stations and airports) that are major hubs for both. These locations demonstrate an interrelationship between the systems and need to be documented.

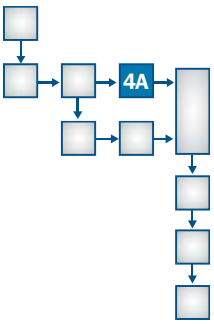
Each separate transportation mode needs to be reviewed to locate and document physical relationships with other systems. Additionally, the same effort is required for the institutional and process layers of each system. Through this effort, an accurate depiction of the current transportation network will be established and available for analysis in the context of the SRO.

3.5.3 Baseline System Performance

Creating a complete baseline model or configuration is a key product of step 3A. Simply stated, the baseline configuration will capture a "rendering of the system"—a depiction of how the system performs under normal conditions. Key to the SBRM's analytical approach, this configuration will enable the sector to understand the impact of specific scenarios (e.g., loss of assets or nodes) on system-wide performance and will facilitate the development of countermeasures in step 4A.

Expert judgment, historical data, and various analytical models will most likely provide baseline calculations. It is important to note that the breadth and comprehensiveness of baseline models will vary depending on the system under study and on the complexity of its associated layers. A complete model is not required to move into the ensuing system assessment step.

3.6 SBRM Step 4A: System Assessment



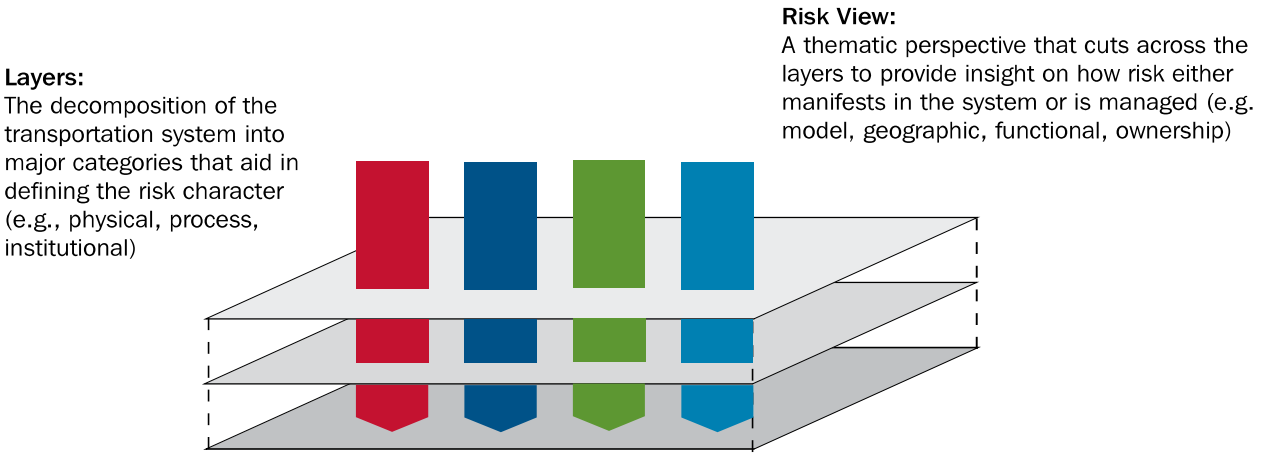
Assessments at the system level are a key component of the sector's SBRM methodology. These assessments assist in identifying and prioritizing risks for infrastructure owners and operators, as well as the government. The SBRM System Assessment identifies, models, and evaluates the effectiveness of countermeasures in targeting systemic vulnerabilities that help the sector achieve SROs. Step 4A involves three main substeps:

1. Analyze system performance and develop countermeasures at the system level;
2. Assess the effectiveness of countermeasures through countermeasure effectiveness modeling; and
3. Finalize a list of proposed system countermeasures.

3.6.1 Analyze Performance and Develop Countermeasures

Even with the informed filtering done in step 2, the baseline representation of the system of interest from step 3A contains a near infinite set of conditions that could be considered. The purpose of this substep is to focus the attention of the detailed analysis on the vulnerabilities (or, more accurately, the perceived weaknesses) in the system that would have the greatest potential impact relative to the SRO if exploited. Three risk layers—physical, process, and institutional—all add to overall system understanding and inform countermeasure options (see figure 3-6).

Figure 3-6: Risk Layers in the Transportation Systems Sector



- **Physical.** The physical level comprises the material components or assets necessary for the continuous operation of the transportation system. For example, the physical components of the rail system include stations, rail cars, tracks, and switches.
- **Process.** The process level comprises the rules, actions, and decisions that give life to the physical level and are necessary for efficient and effective operation of the transportation system on a daily basis. This level captures the ways in which assets work together—physically or virtually. In some cases, these systems may be physically distant from the action they direct. For example, again using the rail system, the process level includes how a particular railroad entity educates its employees and regulates their activity in relationship with established routing guidelines for moving between stations.
- **Institutional.** The institutional level comprises the policy and guidance that empower and constrain the operation of the transportation system to meet the large-scale public objectives essential to long-term sustainability. This includes Federal legislation, national policies, State regulations, and workforce policies. To complete the rail example, the Federal Railroad Administration (FRA) administers track safety standards that govern the building, usage, and maintenance of rail track. Additionally, USCG maritime security regulations, the National Strategy for Critical Infrastructure Protection, State Security Directives, and on-site training or security policies are all part of the institutional level.

A key element of this substep is to identify the primary focus of the system assessment (i.e., system vulnerabilities) and consider possible ways to counter them. Using system/network analysis techniques to assess the system-wide consequences, potential countermeasures are developed. These countermeasures are considered in the context of the SRO-specific analysis criteria

and more generalized consequence criteria derived from the NIPP. In addition, this element examines system-wide threats and uses qualitative techniques to develop potential countermeasures to threats to the system.

3.6.2 Assess Effectiveness of Countermeasures

Countermeasure effectiveness modeling is conducted to see what impact the countermeasures have on the system and assists in making a determination of which countermeasures are worth pursuing based on the positive effect on key performance measures.

Countermeasures are, of course, intended to enable the system to reach adequate performance measures, as outlined by the SRO. Therefore, potential countermeasures need to be evaluated in the context in which the system will operate—namely, a nonlinear and interdependent, multi-faceted threat environment. Moreover, many of the potential countermeasures will themselves depend on the ability to assess their value as it relates to managing systemic effects. All of this points to the need to perform consequence modeling using nonlinear analysis techniques and models. For example, this substep may use the following two modeling methods:

- System Dynamic Modeling is an approach to understanding the behavior of complex systems over time. It deals with internal feedback loops and time delays that affect the behavior of the entire system. What makes using System Dynamics different from other approaches to studying complex systems is the use of feedback loops and stocks and flows. These elements help to capture the nonlinearity of a system using the relationships of the components as the basis of the model.
- Agent-Based Modeling is a specific individual-based computational model for computer simulation extensively related to the theme in complex systems, emergence, Monte Carlo Method, computational sociology, multi-agent systems, and evolutionary programming.

These models could be used to assess how the complex systems perform under changes imposed by the countermeasures.

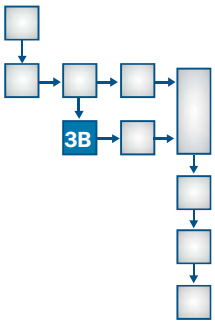
3.6.3 Finalize List of Proposed System Countermeasures

After determining the effectiveness of each proposed countermeasure and settling on the best candidates, the last substep of 4A is to assess countermeasure feasibility constraints and key considerations. This analysis will inform step 5 (prioritization) and step 6 (countermeasure program development) of the SBRM process. While the effectiveness is a key element in determining the sector's portfolio of countermeasures to accomplish SROs, additional factors must be considered. Likely constraints and considerations include:

- **Internal Government Cost.** How much would it cost Federal, State, and local governments to implement this countermeasure?
- **Cost to Industry.** What economic impact could implementing this countermeasure package have on transportation stakeholders?
- **Level of Confidence in Countermeasure.** How much does the projected countermeasure package's effectiveness depend on assumptions? What is the confidence level that the projection is accurate?
- **Likelihood of Success/Difficulty.** Is the package a long shot, but with a very high payoff if successful? Does the package have minimal impact, but is very easy to achieve?
- **Sector Capability.** Is the sector capable of executing the countermeasure package?
- **Time to Implement.** How long will it take to implement the countermeasure? How soon can the first countermeasure begin?
- **Privacy Implications /Legal Considerations.** Are there clear implications with regard to privacy associated with the countermeasure? Any hidden implications? What other possible legal implications exist—regulatory, reporting, conflicts of jurisdiction, etc.?

A cadre of experts throughout the sector will be assembled to evaluate each countermeasure's constraints and considerations. For instance, while financial analysts will be well positioned to ascertain the option's cost to the sector, the same analysts may not have the vantage point to render an opinion on the sector's capability to execute the option. In addition, a wide array of physical, process, and institutional experts will also be required to assess their level of confidence in the predicted effectiveness of each countermeasure.

3.7 SBRM Step 3B: Asset Screen



For each system that is screened in, individual component assets will be identified for examination. The benefits of this approach are a clear connection between the risk objective, the supporting system, and the asset. This approach recognizes the context-specific nature of criticality and helps to reach a point where asset criticality can be demonstrated.

The SBRM asset screen serves as a filter to identify and characterize the most critical assets relative to the SRO. To that end, this step relies on a high level of consequence, or the worst reasonable damage that an asset could suffer as a result of being attacked by a terrorist or being exposed to a natural disaster, to make decisions about which elements of the network are studied in further detail.

This ability to provide context adds a new dimension to the options the sector has in prioritizing actions in response to the materiality of a risk.

3.7.1 Identify Assets

Step 3A will identify the system of interest, but that system is made up of nodes and links that are effectively the assets that need to be examined. The input from step 3A needs to be translated from the context of systems (which step 3A focuses on) to the context of assets. So, the first substep in 3B is to determine the elements that comprise the system under study from step 3A of the SBRM process by taking the system configuration and documenting the nodes and links as assets.

3.7.2 Filter Assets for Criticality

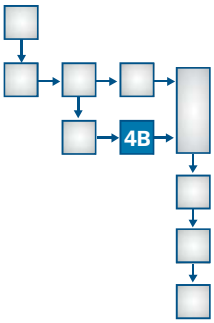
The second substep in 3B is to determine the worst reasonable damage that an asset could suffer or cause as a result of being attacked by a terrorist or being exposed to a natural disaster. By understanding the damage, or consequences, that could be inflicted on any given asset, the sector will ultimately have a more thorough understanding of where to focus its risk analysis activities and associated countermeasures. Historical evidence and other qualitative analysis methods can be used to develop the consequence scenarios.

To fully understand the worst reasonable damage that can be caused to an asset, a number of consequences may need to be evaluated to determine their relative impact. Four key indicators provide a qualitative measure of the impact of each consequence. These consequence criteria are assessed subjectively and include:

- Health impacts;
- Economic impacts;
- Mission impacts; and
- Public confidence impacts.

A rating index will be used in this step to determine which assets will be studied further. Those assets with associated consequences that meet or exceed a predetermined threshold will be selected.

3.8 SBRM Step 4B: Asset Assessment



The SBRM Asset Assessment deploys an analytical approach that seeks to develop countermeasures to reduce the risks to those assets that are critical to the sector's SROs. To that end, step 4B involves three main substeps, which are described in detail later:

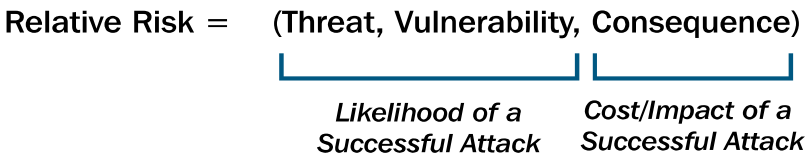
1. Consolidate assets;

2. Evaluate threats, vulnerabilities, and consequences (TVC) against each asset; and

3. Develop countermeasures at the asset level.

The SBRM Asset Assessment is similar to other risk assessments in that it estimates the chances of a specific set of events occurring and/or their potential consequences.[149] Risk assessments carry a range of interpretations that vary within industries. Also, the fundamental understanding of what properly constitutes the risk assessment process can vary.[150] In the context of homeland security, risk assessments typically focus on threats, vulnerabilities, and consequences (TVC), as shown in figure 3-7.

Figure 3-7: Relative Risk as a Function of Threat, Vulnerability, and Consequence



Separate analyses are associated with each term (e.g., threat analysis and vulnerability analysis). A set of activities represent the TVC analyses and are inputted into a resulting risk assessment model. The output of a risk assessment model provides a relative scoring, either qualitative or quantitative, for the assets under study. Today, several agencies have developed risk assessment models that evaluate the TVC functions of the risk equation. Among some of these models are Analytical Risk Management (ARM), Maritime Security Risk Assessment Model (MSRAM), and Risk Analysis Methodology for Critical Asset Protection (RAMCAP).

Step 4B evaluates risk to the critical assets from steps 3B and 4A through a systematic TVC analysis. This risk assessment enables the development of outcome-focused countermeasures designed to reduce the overall risk to the assets under study. Furthermore, since step 4B is an asset-focused component of the larger SBRM, some of the assets requiring countermeasures as a result of the system assessment in step 4A are modeled to determine their effectiveness relative to the performance of the system under study.

3.8.1 Consolidate Assets

Step 4B examines, in detail, the assets that support the SRO. Assets that fit this category come from two primary sources in the SBRM—steps 3B and 4A. In addition, recognizing that these sources may not be collectively exhaustive in terms of critical assets, additional assets must be accounted for and included based on expert judgment. The first element in this activity is to pull the sets of assets from these sources and create a master list of assets that will be examined.

[149] "Risk Analysis," *Social Science Encyclopedia*, Kunreuther, 2004.
[150] A.J. Ignatowski, Ph.D.; I. Rosenthal, Ph.D.; L.D. Helsing, Ph.D., *An Internet Thesaurus/Dictionary for Analyzing Risk Assessment Processes, Laws, and Regulations*, 1997.

3.8.2 Evaluate Threats, Vulnerabilities, and Consequences Against Each Asset

Step 4B focuses on systematically analyzing specific TVC for each asset. Identifying threats and their likelihood enables a thorough understanding of the potential threats that may negatively impact assets. Vulnerability analyses build on this understanding by providing an assessment of security weaknesses that would allow certain method target pairings to succeed, providing the necessary information to determine the likelihood of success for *specific* threats. Finally, an asset's consequence analysis describes the potential results, or impacts, of a threat successfully penetrating any given asset.

After defining threats and analyzing asset vulnerabilities and the possible consequences to an asset, a risk model is used to calculate the overall risk to the asset. The risk calculation is a function of the TVC scores. This aggregated value provides a relative score that can be used to compare each asset.

For the purpose of this analysis, risk is calculated for each asset and compared relative to the score of the other assets.

3.8.3 Develop Countermeasures at the Asset Level

The previous substep provides the processes necessary to develop a comprehensive risk score for each asset. Following this calculation, additional analyses are required to determine those assets that are out-of-bounds with regard to the acceptable risk range. These assets need to be identified, reviewed, and provided countermeasures that can reduce their risk score to a more acceptable range. The candidate countermeasures associated with step 4A, System Assessment, while beneficial for the asset, are input back to step 4A for additional consequence modeling.

3.9 Supporting Activities for Steps 3 and 4

Asset-level assessments are performed at multiple levels and by various stakeholders.

3.9.1 Government Asset-Level Assessments

Federal assessors across the various modes and agencies conduct a comprehensive program of scheduled on-site facility security assessments and inspections to evaluate facilities based on risk and regulation. Their focus is on assessing risk to "highly critical" assets and systems, specifically those areas that fall outside the responsibility of the private sector.

The sector uses these assessments to review and verify infrastructure data, which may be shared among Federal partners. Using a wide variety of general and mode-specific assessment tools, assessors evaluate TVC and existing security measures. The assessment team provides a formalized report that will be reviewed with executive-level site managers. TSA captures results from assessments as lessons learned or best practices to assist the efforts of other stakeholders with similar vulnerabilities. The lead Federal security partner in charge of the assessment shares the results with TSA for further analysis.

3.9.2 Facilitated Asset-Level Assessments

These assessments enable State, local, tribal, or private sector stakeholders to use government assessment tools, training, and technical expertise to assess their infrastructure. The goal is to build capacity beyond the Federal Government for owner/operators to effectively assess their risks and aid the sector in acting on that information. Facilitated assessments offer increased access to accurate assessment data, improved comparability by using standard government tools, and opportunities to build relationships with owner/operators. TSA will capture the results from assessments as lessons learned or best practices to assist the efforts of other stakeholders with similar vulnerabilities. Finally, the lead Federal security partner in charge of the assessment will share the results with TSA for further analysis.

3.9.3 Owner/Operator Asset-Level Self-Assessments

State, local, tribal, and private sector stakeholders will also conduct assessments of their infrastructure according to their own needs or as required by law. These assessments will focus primarily on the vulnerabilities unique to the infrastructure for which they have responsibility. As a component of the top-down/bottom-up approach discussed in section 1, these assessments aid in criticality screening.

In addition to securing their facilities in the name of insurance or business continuity, stakeholders may also demonstrate national pride and civic obligation to protect their workforce, communities, and customers by completing assessments. The Federal Government will support State, local, tribal, and private sector leaders by engaging in an effort to communicate, publicize, and encourage the use of risk assessments regardless of whether the data are ever shared beyond the fence line of the owner/operator.

Assessments within this owner/operator community are not tied to using any one tool or methodology, but instead may rely on the tools and methodologies best suited to their unique needs. For those new to the sector, or new to conducting risk assessments, the SCC may provide a list of recommended best practices, tools, and methodologies. Additionally, the Federal Government will provide access to appropriate Web-based tools for assessments, as well as educational materials on the definitions of consequence, threat, and vulnerability.

3.9.4 Assessments for Cyber Networks

The cyber networks supporting the transportation system are very similar to the other systems under consideration. However, the accessible and networked nature of the cyber infrastructure results in an environment prone to internal threats, external attacks, and human error. Cyber threats are constantly evolving, with attacks by non-traceable actors that do not necessarily conform to historical event patterns. Based on these factors, it is in the best interests of sector stakeholders to focus on cyber risk assessment as a distinct effort.

NIST, the Information Systems Audit and Control Association (ISACA), the International Organization for Standardization (ISO), and a number of other organizations have documented and distributed detailed technical checklists, risk assessment checklists of controls, and information security management systems best practices. Based on regulatory requirements, sector members from the Federal, State, and local levels are often required to use the NIST *Self-Assessment Guide for Information Technology Systems*, Special Publication (SP) 800-26 and the NIST *Recommended Security Controls for Federal Information Systems*, SP 800-53 to assess levels of vulnerability and risk.

The private sector will be encouraged to use the Control Objectives for Information and Related Technology (COBIT) methodology, which is sponsored by ISACA. The COBIT methodology is aimed at assessing management standards, and may be used in conjunction with the NIST assessments commonly used by the Federal Government or NIST eScan,[151] which was developed for the private sector. Sector partners are encouraged to report security incidents to the United States Computer Emergency Readiness Team (US-CERT).

International partners will be encouraged to use the assessment methodologies referenced above, or ISO 27001 and ISO 17799, which are intended to be used together.

[151] The NIST eScan Security Assessment is a diagnostic tool designed to assess the electronic security infrastructure of a small business and provide an action plan for improving it. This tool will provide a set of recommendations to correct security problems, and will help develop a more secure model for future eBusiness strategies and positioning.

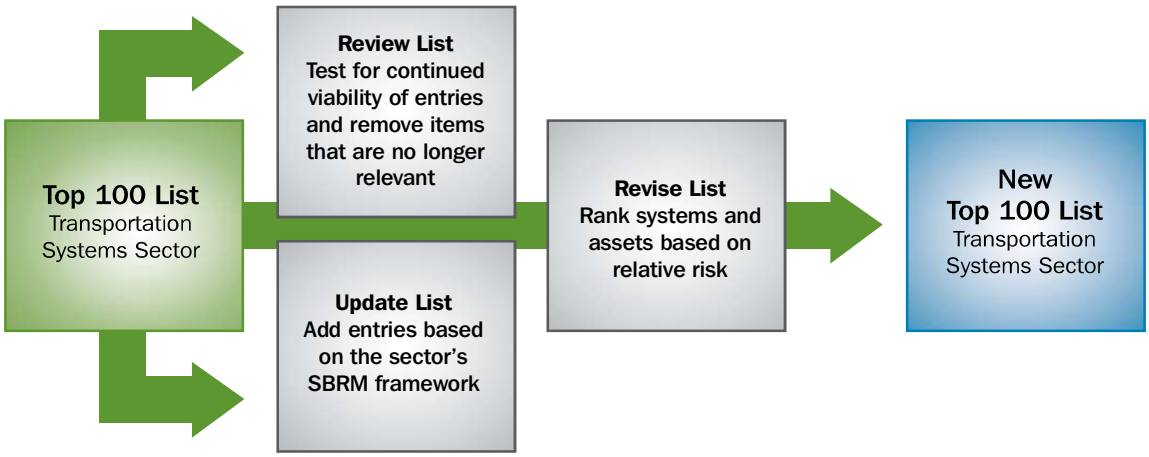
3.9.5 The Top 100 List

In fiscal year (FY) 2005, the DHS IP requested sectors, including the Transportation Systems Sector, to develop Top 100 asset lists, which served as a Buffer Zone Protection Program (BZPP) decisionmaking tool. With the addition of systems and networks in the NIPP, it is expected that the future content of this list will expand to include many system entries.

SBRM includes an element that focuses on annually updating the sector's Top 100 list. The update will be based on the insights developed through the implementation of the SBRM process. Specifically, the process for updating the list will use the previous year's list as a starting point. The list will be reviewed to include updated information from the SBRM process to help guide the sector's decisionmaking process. Entries that are no longer at a high enough relative risk level to warrant the continued attention that the Top 100 list provided will be removed.

The major steps involved in updating the list are presented in figure 3-8.

Figure 3-8: Substeps to Update the Top 100 List



As shown in the figure, the first substep is a completed scrub of the existing list to check for entries that can be removed. This could be for any number of reasons, but the decision to remove an entry must be done with a clear indication of the rationale for the decision. The scrubbed list is then used as the basis for additions derived from the SRO-driven analysis.

SBRM steps 3B and 4B will result in the identification of assets within the national transportation system that are critical to a given SRO. In many cases, these assets will already be included in the Top 100 list, but in the event that a different asset is identified through the process, it will be considered a candidate to be included in a revised Top 100 list.

In addition to the assets, the SBRM process will identify critical systems and networks. SBRM steps 3A and 4A will result in the identification of the networks and systems associated with the SRO. All of these systems and networks will be considered as candidates to be included.

After the candidate asset, systems, and networks are identified, they will be ranked by relative risk. To do this, a heuristic rule set will be applied to decide whether to include the asset on the list, or to include the larger system within which the asset resides. The entire system belongs on the list if:

- Countermeasures are more aptly applied across the entire system to mitigate the risk as opposed to just at the critical asset(s).

- There are many assets related to greatest risk(s) versus a small number of critical assets within the system. For example, if the risk is associated with an improvised explosive device (IED) killing passengers on a train, there are a large number of places within the train where that can take place. Assuming there aren't a few places where the deaths are much higher (like in an underwater tunnel), it makes more sense to place the entire system on the list rather than each passenger station/train car.
- The risk scenario being considered involves attacking the entire system (e.g., the Mississippi River bridge system) as opposed to a single asset (e.g., a single bridge along the river).

Alternatively, a single asset belongs on the list if:

- It is the critical node within the system.
- Countermeasures would generally be applied at the asset, not the system.

4. Prioritize Risk Management Options

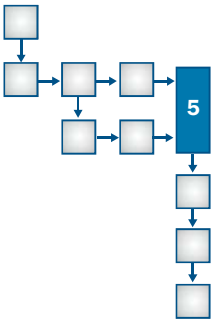
4.1 Introduction to Prioritization

While the Federal Government continues to make significant investments to improve transportation security, it is not possible to eliminate all the vulnerabilities from all transportation systems throughout the country. The uncertainty of system behavior means that perfect security is not possible. Therefore, it is essential to make strategic improvements based on prioritized risk management options according to system risk.

The first step in prioritizing risk is acknowledging that the sector's approach to risk must be system-based. Such an approach calls for a systematic decision process by which the cost, time, and other characteristics of potential solutions (along with the potential impact to the network) of the various mitigation and countermeasure options available are compared and contrasted. This analysis enables decisionmakers charged with protecting the transportation network's security to prudently develop strategies, investments, actions, and resources to effectively manage risk. After developing solutions, strategy must be effectively translated to action. Stakeholders must evaluate the sector's portfolio of programs effectively by rigorously tracking cost, schedule, and performance to ensure success.

The sector-wide analyses and prioritization are in no way intended to remove the budgetary discretion of individual agencies in managing their budget. Among agencies across the sector, determinations and prioritizations on which security programs merit additional funding shall be advisory in nature, and considered along with other priorities within each agency's budget development process.

4.2 SBRM Step 5: Countermeasure Prioritization



The countermeasures that emerge from steps 4A and 4B have been scored and ranked according to their effectiveness against the SRO. However, these rankings alone do not result in effective, cost-efficient solutions. The interactions and net effects of countermeasures must be considered before strategies can be translated to effective action plans. For example, if one highly ranked countermeasure from step 4A overlaps with, or even negates, another highly ranked countermeasure from step 4B, its collective effectiveness will decrease. Alternatively, a package that incorporates countermeasures that are complementary to each other could result in an increased collective effectiveness at a reduced cost.

As a result, in step 5, working groups are formed to identify ways that effective countermeasures can be packaged together to achieve the SRO. Once these countermeasures are identified, the working group will score and rank each package's cost and overall effectiveness. These comparative rankings will allow the sector to identify the countermeasure packages that experts have judged to be most

effective in helping decisionmakers build balanced, focused, high-impact countermeasure programs in step 6. The three main substeps associated with step 5 are:

1. Develop decision framework;

2. Package countermeasures; and

3. Rank countermeasure packages.

4.2.1 Develop Decision Framework

The first substep in step 5 is to select experts to develop the decision frameworks necessary to identify and prioritize countermeasure packages. It is essential that these working groups are composed of a knowledgeable and diverse cadre of subject matter experts to evaluate the array of potential countermeasure packages. Next, a method to rank the packages, taking into consideration the relative importance of each in achieving the SRO, will need to be established.

4.2.2 Package Countermeasures

Before the new countermeasure packages are identified, the sector must identify existing efforts that may contribute to SRO achievement. These existing efforts may be incorporated into countermeasure packages to ensure that the packages balance existing activities with the introduction of new ones. This means existing efforts may require replacement or elimination if their performance no longer supports the agency's priorities.

The working groups will assemble well-informed packages by analyzing countermeasure synergies, redundancies, timing issues, and other considerations. It is important that countermeasure packages are developed to address the entire portfolio associated with the SRO. Furthermore, at this point in the process, it is also necessary to consider a variety of different packaging strategies, as an evaluation of constraints and other considerations may drive the need for an analysis of a wide array of potential solutions.

4.2.3 Rank Countermeasure Packages

After establishing the decision framework and developing the packages, experts must evaluate the relative impact of each countermeasure package against the SRO and estimated cost to implement.

It is essential that the established working group possess the domain and functional expertise necessary to make well-informed judgments. For example, countermeasure packages seeking to mitigate risk through institutional (e.g., regulations) and process changes may require a different set of experts than those aimed at improving the physical integrity of assets.

The first step in the scoring process is to determine the relative effectiveness of each countermeasure package. Surveys, voting, discussion, and consensus among experts may be helpful to make well-informed decisions.

Next, the estimated cost to implement must be evaluated. While it is necessary to assign cost scores to countermeasure packages, detailed cost analyses are not required at this point in the SBRM process. Finally, once the effectiveness and cost scoring exercises have been completed, the countermeasure package scores are adjusted according to the SRO.

Once these scores are calculated for the countermeasure packages, a review committee will verify the scores that were given to the countermeasure packages. The verification process ensures that any "groupthink" that might emerge from working group sessions is corrected.

When the scores are verified, a ranked, prioritized list of countermeasure packages will be compiled. While these effectiveness rankings are useful for identifying cost-effective countermeasure packages, they alone cannot determine which countermeasure packages should be incorporated into programs. Key considerations and constraints must be evaluated.

4.3 Support Activity for Step 5

Although the cyber risk management prioritization process fits within the SBRM framework, the unique challenges of cyber risk require specific mention.

4.3.1 Cyber Prioritization

Sector members will be responsible for performing prioritization of critical cyber assets and reporting relevant metrics as requested by sector working groups. Stakeholders should utilize NIST Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems,* which provides guidance for prioritization and addresses a tiered approach to segment the items into high, medium, and low categories.

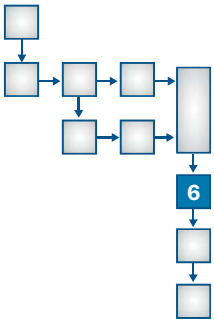
5. Develop and Implement Security Programs

5.1 Overview of Sector Security Programs

In the wake of September 11, 2001, security measures implemented across the sector were selected using a variety of approaches. For example, the freight rail industry conducted a vulnerability and risk analysis using Federal Government, industry, and international best practices. The result of this effort was the Railroad Terrorism Risk Analysis and Security Management Plan. Simultaneously, individual owner/operators began implementing a variety of security programs or individual security measures, sometimes based on widely accepted risk assessment methodologies.

Building on earlier efforts, all sector security partners will continue working together to develop an overarching portfolio of risk-based security programs and countermeasures to improve the sector's risk profile. TSA will facilitate the development and implementation of security programs by coordinating with stakeholders through the GCC and SCC to manage risk by minimizing consequences, mitigating vulnerabilities, and deterring threats. Each partner is responsible for developing protective programs that are risk-based, coordinated, scalable, and cost-effective to their individual organizations. TSA will work with the DHS NCSD to ensure that the sector partners are informed about available cyber protection program methodologies.

5.2 SBRM Step 6: Countermeasure Program Development



In step 6, the prioritized countermeasure packages that emerged from step 5 will be scored according to their overall value and organized into balanced, focused countermeasure programs. The overall value of such programs is determined by comparing the effectiveness scores from step 5 to the constraints and considerations that may impact each program's effectiveness, such as organizational capability, internal cost, and time to implement. Once completed, the sector will conduct a top-down review of the programs to ensure that other factors, such as stakeholder concerns, are considered and incorporated into the final set.

In short, the countermeasure program refinement and vetting process allows sector management and decisionmakers to ensure that the programs are focused, realistic, and aligned with strategic management considerations.

5.2.1 Assess Constraints and Considerations

A well-informed selection of countermeasure programs requires a complete understanding of the costs, constraints, and considerations associated with their implementation.

One of the most important constraints impacting countermeasure packages is available funding. As a result, step 6 begins with identifying SRO budget ranges. These ranges will be an important factor in the portfolio optimization process.

The second substep is assessing other key constraints and considerations affecting countermeasure program value. In step 4A, a high-level analysis of constraints was conducted for each countermeasure. As previously stated, constraints and considerations could include:

- Internal government cost;
- Cost to industry;
- Level of confidence in countermeasure;
- Likelihood of success/difficulty;
- Sector capability;
- Time to implement; and
- Privacy implications/legal considerations.

To assess these constraints and make judgments on their impact on program effectiveness, working groups will create a framework to guide the constraints analysis. This framework will state what types of constraints and considerations should be assessed. For example, a particularly sensitive SRO to prevent terrorist attacks on critical systems could include countermeasure packages that might raise privacy concerns from citizens or sector stakeholders. As a result, this constraints analysis framework may include privacy as a key consideration to be assessed.

Once key constraints categories are determined, the working group will assign relative weights to each. These weights should reflect the requirements of each SRO. For example, a particularly time-sensitive SRO might place a high weight on the length of time required to implement.

With the constraints analysis framework finalized, the working group will assess the factors impacting each countermeasure package's effectiveness. To conduct the analysis, the working group will consider expert opinion, historical data, and feedback from strategic sources.

Once these constraints and alternatives are documented, the working group will determine the degree to which the constraints impact countermeasure package effectiveness. Similar to the scoring in step 5, a number of methods—surveys, voting, discussion, and consensus—can be used to conduct the scoring exercises.

The scores that result from this exercise will be aggregated and weighted for each countermeasure package. The sum of the constraints scores can then be evaluated against the effectiveness rankings developed in step 5. The sum of the two can be described as the countermeasure package value.

5.2.2 Build Countermeasure Programs

Countermeasure programs should consist of groupings of countermeasure packages that are thematically linked and their collective impact is sufficient to substantially meet SRO goals. The first activity in building countermeasure programs will be to align the countermeasure packages with the highest value to the SRO that they were designed to achieve. Next, the overall impact of constraints and considerations will need to be evaluated to determine each package's feasibility. Those packages perceived to be the most effective in accomplishing the SRO may need to be augmented to address the constraints evaluated earlier in the process.

5.2.3 Review Countermeasure Programs

Once the SRO countermeasure programs are developed, sector leadership will conduct a top-down review of the recommendations, taking into consideration management perspectives. It is important to note that the analyses supporting the proposed programs provide an overarching framework for decisionmakers, but do not substitute experience and institutional knowledge. For example, it may be determined that even though the sector does not currently have the organizational capability to implement a very costly, but potentially effective countermeasure package, the positive effects of that countermeasure package outweigh those constraints and it should be included in a countermeasure program. Alternatively, it may be determined that a countermeasure program would have such a significant negative impact on sector stakeholders that it should not be implemented, or that additional activities will be necessary to mitigate the negative impact.

The high-level review finalizes the portfolio optimization step and sets the stage for planning and deployment activities in step 7.

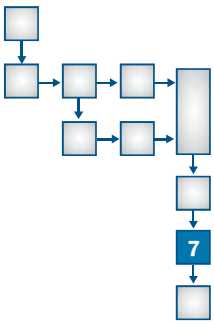
5.3 Supporting Activities for Step 6

Once assessment and prioritization of risks have been completed, a gap analysis will be performed between identified needs, existing security programs, and progress toward achieving sector security goals.

Discussion of the Risk and Strategy Matrix (RASM) provides the necessary structure to ensure that the Transportation Systems Sector is effectively making progress toward measurable outcomes. RASM assists in gap analysis by helping to inform the sector as to whether the SRO has adequate security measures across the set of sector goals.

GCC and SCC partners will 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, TSA will lead an examination of other programs (including grants) that may be adapted to address the need or direct R&D activities to design new capabilities. Because of the likelihood that potential risk gaps may involve areas where numerous interdependencies are present, TSA will work with other sector lead agencies to identify and leverage potential programs as warranted.

5.4 SBRM Step 7: Deployment Engine



In step 7, the SRO countermeasure portfolios that emerged from step 6 are transitioned into sector planning and budgeting activities. To achieve this alignment, countermeasure program plans are developed that outline the roles and responsibilities necessary to resource, manage, and oversee their implementation.

These alignments provide stakeholders with a clear link between their respective program portfolios and the sector's SROs. This link will be further detailed in step 8, as measures are developed that assess the degree to which countermeasure programs are contributing to SRO achievement. The following substeps align with the Federal Government's Planning, Programming, Budgeting, and Execution (PPBE) activities. It is important to note that the process described below is not intended to replace the existing budget processes of sector stakeholders, but rather relate SBRM methodology, specifically SROs, to their current budgetary planning activities.

5.4.1 Develop Program Plans

The countermeasure programs that emerge from step 6 indicate the investments that the sector has determined will be most effective in supporting achievement of the SROs. Simply stated, while these programs indicate *what* needs to be done, they do not describe *how* to do it. As a result, the initial substeps in step 7 focus on creating plans that describe the activities necessary to initiate and implement the countermeasure programs and coordinate responsibilities within the sector.

Program plans will outline which stakeholders are likely to have management responsibility and authority to oversee countermeasure program implementation and to what degree the programs will require coordination with Transportation Systems Sector security partners. They will also provide the budget estimates for activities under the countermeasure program and their respective implementation milestones. In addition, the program plans will also detail specific activities necessary to mitigate the implementation constraints identified in step 6 of the SBRM process.

5.4.2 Coordinate Program Plans

At this point, the program plans are initial projections of who will be responsible for managing and overseeing countermeasure program implementation. Coordination between sector partners is key to ensuring that program plans avoid duplicative or conflicting countermeasures, define clear roles and responsibilities, and drive collaborative efforts.

5.4.3 Integrate Program Plans Into Budgeting Processes

Each security partner (Federal, State, and local governments, and the private sector) has its own unique budgeting process for determining, rationalizing, and approving funding levels for security programs and initiatives. In this substep, the Federal budgeting processes will determine appropriate funding levels for its programs and initiatives. Once Federal funding levels are determined, decisions can be made on how to allocate available Federal resources and used to inform the State, local, and private sector budgeting process. If budget gaps are identified, decisions should consider the criticality of the countermeasure programs to accomplishing the SROs and the impact that a gap in countermeasure program funding would have on SRO achievement.

As a result of step 7, sector strategies and budgets will be aligned and integrated with the sector's highest priorities. This integration allows sector stakeholders to clearly understand, at a high-level, how their organization and operation unit portfolios impact and link to countermeasure programs and SRO aims. This understanding of program/SRO alignment is critical to step 8, in which performance measures are developed that detail how countermeasure program implementation contributes to SRO achievement.

The sector-wide analyses and prioritization are in no way intended to remove the budgetary discretion of individual agencies in managing their budget. Among agencies across the sector, determinations and prioritizations on which security programs merit additional funding shall be advisory in nature, and considered along with other priorities within each agency's budget development process.

5.5 Support Activities for Step 7

A number of existing programs and activities will act as key sources of information for the overall SBRM process. The supporting activities listed below remain essential tools in the deployment process.

5.5.1 Cyber Programs

Sector partners are responsible for implementing their own cyber security programs. TSA will coordinate through the GCC and SCC communities and with NCSD to provide online, annual, in-person forums for sector members to share their best practices in IT security and other security programs. The SCC will play a key role in communicating and implementing new programs to ensure the resilience of transportation cyber networks.

TSA coordinates efforts with US-CERT through notifications of incidents affecting TSA and by reviewing bulletins distributed by US-CERT. Other Federal partners and the private sector are encouraged to take advantage of the information shared by US-CERT.

TSA meets with NCSD and the Chief Information Security Officers (CISOs) from various government agencies to develop best practices. TSA will continue to work with NCSD to ensure that TSA and the sector's cyber protective programs are aligned with NCSD's goals for the IT sector and follow best practices developed by NIST and the ISO.

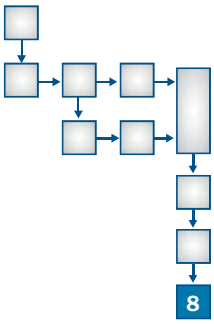
The cyber protective programs recommended in this section are intended to be used as self-assessments. Many of the programs result in an executive report or summary data that is analyzed by cyber security professionals. To measure protective programs, stakeholders will be asked to share their baselines, their performance goals, and their ability to achieve performance goals. For stakeholders who may need more guidance in this area, TSA will coordinate with NCSD to develop a list of recommendations and points of contact that can provide additional guidance.

5.5.2 Security Program Maintenance

Maintenance of security programs—and their continued contribution to the sector's resilience strategy—is a shared responsibility. Duties associated with this responsibility will vary with the security program and the scope of the program's goals. Maintaining federally operated and managed programs is the responsibility of the designated lead Federal partner. If the security program is developed and managed at a regional or local level, owners and operators at that level are responsible for maintenance. TSA will coordinate and communicate with stakeholders to ensure that any changes impacting other programs or planning efforts *at any level* are properly explained and efficiently carried out (this may include, for example, grants to State departments of transportation or State Homeland Security Advisors).

The success of any security program is based, in large part, on the input and cooperation of relevant stakeholders. The GCC and SCC will play essential roles in monitoring the success of each program to assess and justify continued maintenance of programs over their life cycle. The councils will work with the Measurement Joint Working Group to ensure that performance measures are reviewed and updated as necessary. The lead Federal partners for each security program will be responsible for providing standardized feedback and conducting an annual survey on the effectiveness and efficiency of their programs. This feedback will be used to guide program continuation or adjustment, as well as to collect best practices and lessons learned in developing new programs.

5.6 SBRM Step 8: Performance Measurement



In the eighth and final step of the SBRM, the sector will identify and implement meaningful performance measures that track the progress and effectiveness of countermeasure programs in achieving the sector's SROs. These performance measures empower stakeholders to track whether their program portfolios are behind or ahead of schedule and observe the degree to which their activities are supporting the achievement of the SRO.

Monitored, collected performance measures also enable executives to communicate progress toward SROs to Transportation Systems Sector security partners and oversight entities. In addition, the findings that result from these measures will lead to continuous improvements in future iterations of the SBRM.

5.6.1 Map Desired Activities, Outputs, and Outcomes for Each Countermeasure

To conduct these evaluations, measures of effectiveness must be developed and monitored for each countermeasure program. These effectiveness measures flow from maps of activities, outputs, and outcomes—also known as performance logic models.

5.6.2 Develop Performance Measures and Data Requirements

Output and outcome performance measures will emerge from developing countermeasure program performance logic models. These measures will be used to monitor the degree to which countermeasure programs are achieving their objectives. Output

measures will assist in analyzing the program's ability to meet the milestones, while outcome measures will gauge a program's contribution to the sector's SROs.

As these performance measures are identified and documented, the types of data that need to be collected to perform the evaluations will also be identified.

5.6.3 Develop Data Collection, Verification, and Reporting Processes

Based on the data requirements identified in the previous activity, the sector will develop a data collection plan for each countermeasure program. The data collection plan should define what data needs to be collected to inform each performance measure, how frequently this data should be collected and, perhaps most importantly, what resources will be required (e.g., analytical tools and methods) to collect the data.

5.6.4 Link Sector Measures

Once the performance measures are identified and data collection plans completed, performance management responsibilities will be agreed to by sector stakeholders. This is particularly important because during the life cycle of a given countermeasure program, output and outcome measures may reveal best practices, improvement areas, and opportunities for management intervention.

The overall measurement of the performance for the Transportation Systems Sector is discussed in detail in section 6, Measure Progress.

6. Measure Progress

6.1 CI/KR Performance Measurement

An effective NIPP performance measurement program begins with the collaborative development of metrics to measure progress and performance. A formal Measurement Joint Working Group, created under both the Transportation Systems GCC and SCC and under the leadership of TSA's lead measurement organization, will operationalize measures, establish data sources, establish data collection and verification procedures, set measurement policy for the Transportation Systems SSP, and approve supporting procedures. The Measurement Joint Working Group will be composed of transportation subject matter experts from each mode, sector risk leaders, sector cyber security leaders, GCC and SCC measurement leaders, private sector data store leaders, and invited measurement professionals.

The Measurement Joint Working Group will communicate regularly with both the GCC and SCC members and will ensure that working group progress and plans are fully transparent and have the cooperation of GCC and SCC members. In addition, work products of the Measurement Joint Working Group will be submitted for approval, when appropriate, to the overarching Transportation Systems GCC and SCC, the DHS, and NCSD. Expected benefits of the group include minimizing the risk in measure selection, promoting measurement efficiency by leveraging existing private and government data stores, promoting cross use of NIPP measures to meet OMB measurement requirements, providing decision-quality information for NIPP Annual Report analysis, and ensuring effective measurement approaches that produce results with the least impact on stakeholders.

6.2 Developing Metrics

6.2.1 Use of Core Metrics Defined by the DHS

The core metrics, common across all sectors, are a set of descriptive and output metrics that measure progress made by all CI/KR sectors in implementing the NIPP risk management framework. The DHS develops the core metrics and communicates them to the SSAs. A sample of the current core metrics reported includes:

- Total number of assets by class (mode);
- Percentage of medium- and high-consequence assets rated as high risk;
- Percentage of formal security partner agreements by sector and geographic location; and
- Percentage of assets reduced from high risk.

The complete list of core metrics is likely to evolve over time and be much larger. The DHS will also identify cyber security core metrics.

6.2.2 Development of Sector-Specific Measures

In addition to core metrics, the Measurement Joint Working Group will develop sector-specific metrics to more thoroughly evaluate sector progress and drive continuous improvement in achieving the goals and objectives determined by the sector.

There are two types of sector-specific metrics:

- Metrics associated with Transportation Systems Sector goals and objectives; and
- Metrics associated with Transportation Systems Sector programs.

Sector-specific metrics also will include both common and tailored cyber security measures. In addition, metrics associated with the SROs within the sector's SBRM methodology will focus on driving continuous improvement of the SBRM process.

6.2.3 Metrics Associated With Sector Goals (Outcome Measures Associated With Sector Goals and Objectives)

The sector-specific measures associated with sector goals and objectives are proposed to be outcome measures. Proxy (interim output) measures may be required as stand-ins for outcome measures in the early years of the program when baseline data are being acquired. The outcome measures will monitor *information on effects*[152] related to meeting sector goals and objectives. The Measurement Joint Working Group will execute the published Outcome Monitoring Technique[153] for each sector goal and objective combination as follows:

Step 1: Working top-down, document the outcome measurement logic model.

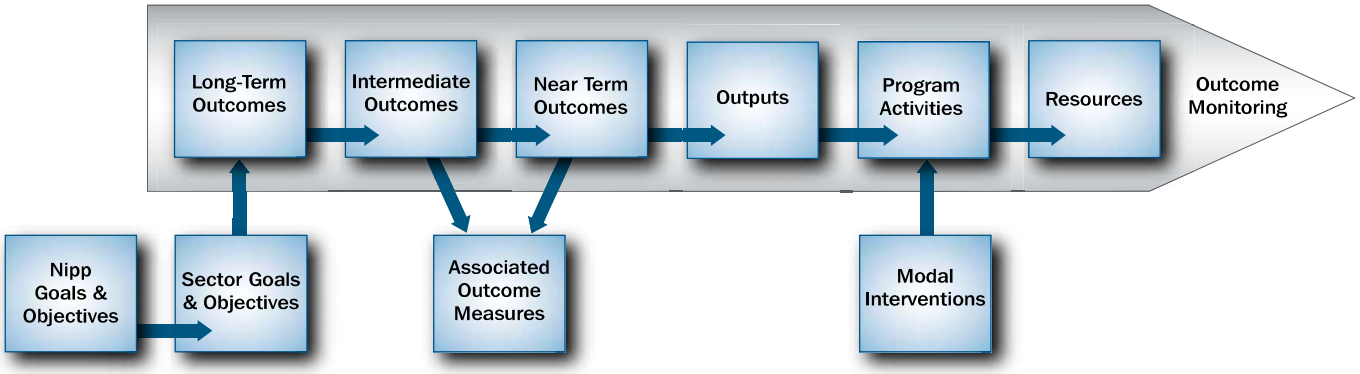
Step 2: Translate near- and intermediate-term outcomes into outcome measures.

Step 3: Operationalize the outcome measures using existing data when possible.

Step 4: Commence ongoing (year after year) measurement.

The steps are captured in figure 6-1.

Figure 6-1: Outcome Measurement Logic Model



[152] In the evaluation literature, measures of effectiveness or *effect* mean how much change can be attributed with some degree of confidence to the concept being measured. Empirical techniques, such as the Randomized Controlled Trial advocated by OMB, are the only program measurement techniques that allow one to determine *with high confidence* the size of an *effect* attributed to an intervention (i.e., program).

[153] For further information on the Outcome Monitoring Technique, see "Measuring and Monitoring Program Outcomes," in Rossi, Peter H.; Lipsey, Mark W., et al., *Evaluation: A Systematic Approach*, 7th edition, Thousand Oaks, CA: Sage Publications, 2004, pp. 203-233. Per Rossi, et al., pp. 224-225, "… [O]utcome monitoring provides useful and relatively inexpensive information about program effects, usually in a reasonable time frame. … Because of its limitations, however, outcome monitoring is mainly a technique for generating feedback to help program managers better administer and improve their programs, not one for assessing the program's effects" on the conditions the program is intended to improve. The Outcome Monitoring Technique, while not empirical, also may be useful for identifying *effect* in areas, such as security, where there are believed to be few competing alternative explanations or interventions.

In addition, for the sector goal *enhance information and intelligence sharing among transportation sector security partners*, the Measurement Joint Working Group will document, for GCC and SCC coordination, how the implementation of this goal and associated objectives will satisfy the requirements of Executive Order 13416, Strengthening Surface Transportation Security. This Executive Order is expected to request annual reviews of the effectiveness of surface transportation system-related, information-sharing mechanisms.

6.2.4 Metrics Associated With Transportation Systems Sector Programs

Each year, both the Transportation Systems Sector GCC and SCC will identify the most significant and innovative programs within the sector believed to have the greatest potential for improving security within the sector. For these model programs, which will be documented in the annual report, the Measurement Joint Working Group will coordinate with program owners to develop and operationalize a program-specific set of measures and reporting schedule. At a minimum, each model program will have one outcome measure, one cost-effectiveness measure,[154] one risk-reduction impact measure, and one efficiency (if required by IP) measure. Additional measures derived using conventional performance measurement (performance indicator monitoring) techniques also are possible.

Included GCC security programs already may be measured as required by the Government Performance and Results Act (GPRA), the Program Assessment Rating Tool (PART), and OMB 300. GCC members will be encouraged to use existing measures to the maximum extent possible, but are permitted to augment existing program measurement practices with incremental practices adopted to support sector annual report requirements, if deemed appropriate by each individual agency.

6.2.5 Strategic Risk Objectives Measures

The Transportation Systems GCC and SCC are expected to request the Measurement Joint Working Group to also measure progress toward meeting selected SROs. SROs derive from the SBRM process and will be defined more fully over time.

6.3 Information Collection and Verification

Information collection and verification can commence once the performance measures are operationalized. Information collection begins with identifying the data owners for each performance measure, the source of the data, the frequency of data collection, metrics assessment process and frequency, and any validation that applies to the performance measure.

Performance metrics will go through a validation and verification process. This process builds on the operationalization data to:

- Validate the data sources from which the data are obtained;
- Fully describe each performance measure;
- Validate methods and frequency for data collection;
- Describe how the data are verified (i.e., how we know that the data are accurate and timely and comparable to data from other time periods);
- State whether the data are reliable and how reliability is measured;
- Establish protocols for the data owners to validate the accuracy of the data provided; and

[154] The cost-effectiveness measure is similar to a cost-benefit measure ("we lowered risk by x and it cost y dollars"). Such knowledge can be used to evaluate performance and prioritize next steps at the NIPP level. Cost-effectiveness measures aid in evaluating whether the most cost-effective process has been employed and ensuring that a project's targets are met.

- Provide a complete set of metadata templates for each performance measure that captures key data points that will serve as the measure data dictionary.

Data collection will be an ongoing process. Following regular data collection, a coordinated higher level review may be conducted by an office not responsible for collecting the data. The SSA's lead measurement organization will serve as the roll-up point for measurement information received from the sector. Although this organization and its systems can handle both unclassified and SSI material, sister organizations (e.g., Risk Management Strategic Planning (RMSP) Division, OI) do handle classified material.

As the measure development, data collection, and verification processes mature, supplemental technology tools (data modeling and verification) might be considered to automate the data accuracy, reliability, and verification procedures. Statistical sampling tools can be applied to provide quantifiable information that supports the accuracy, reliability, and validity of the data supporting each performance measure.

6.4 Reporting Timelines

Core and sector-specific metrics will be reported to the DHS on a regular, predetermined schedule to ensure that they meet the DHS's need to monitor performance across all sectors. To the extent feasible, sector reporting timelines will be established to coincide with OMB and other legislative reporting requirements. The Transportation Systems Sector Measurement Joint Working Group will work with the GCC and SCC to identify, document, and implement the most effective and cost-efficient repeatable process, and establish a schedule to report core and sector-specific metrics (goal and program) to the DHS. SROs also will be reported within the sector to guide the sector's risk management program. Process definition will include evaluation of the most appropriate role for the emerging IP Metrics Web Portal platform in the final sector reporting processes.

HSPD-7 requires SSAs to provide the Secretary of Homeland Security with an annual report on their efforts to identify, prioritize, and coordinate the protection of CI/KR in their respective sectors. TSA worked in close collaboration with sector security partners, SCCs, GCCs, and other organizations in developing the 2006 Annual Report and will continue to do so for further reports. The Measurement Joint Working Group and the Transportation Systems Sector GCC and SCC will work to establish the reporting timeline and measurement requirements to support future Transportation Systems Sector Annual Reports.

6.5 Implementation Actions

The sector's security partners have identified a series of actions to be completed as the Transportation Systems SSP is implemented over the next few years. These actions, illustrated in table 6-1, represent the major actions that TSA and some members of the sector will undertake to achieve a robust, resilient transportation infrastructure. The actions listed in table 6-1 are "notional"—meaning they provide a sense of what will be accomplished over the next few years. The SCC and GCC will identify improved, more definitive milestones through collaborative discussions. Successful completion of these actions depends on the availability of public and private resources.

TSA and USCG, as the SSAs, will work with the Transportation Systems Sector GCC and SCC to undertake the responsibilities included in table 6-1. Unless otherwise stated, all milestones will be targeted in cooperation and coordination with all transportation security partners under CIPAC, including, but not limited to, TSA, the Transportation Systems Sector GCC and SCC, the DHS, and other security partners in government and industry.

Table 6-1: Milestones of Key Responsibilities Under HSPD-7

Milestone	Date	Lead Responsibility
Establish sector partnership coordination processes to ensure that all security partners (Federal, State, regional, local, and private sector) are involved in planning efforts from their inception.	No later than (NLT) 30 days after SSP submission	SSAs
Establish process to introduce NIPP implementation actions according to appendix 2B of the NIPP.	NLT 90 days after SSP submission	GCC/SCC
Continue to build and strengthen the role of the GCC and modal GCCs, the modal SCCs, CIPAC, and its transportation security committees and working groups to implement the Transportation Systems SSP, the modal implementation plans, and related security activities.	Underway; ongoing	GCC/SCC
Continue and expand on joint exercises with transportation security partners and other interdependent sectors.	Ongoing	GCC/SCC
Enhance information-sharing platforms, such as HSIN and ISACs, to share information on threats to the transportation infrastructure and security partners.	Ongoing	GCC/SCC
Develop an ongoing process for assessing compliance with any security guidelines and security requirements issued by the Secretary of Homeland Security or Secretary of Transportation for surface transportation systems and the need for revision of such guidelines and requirements to ensure their continued effectiveness.	Underway; ongoing	SSA
Convene a technical assistance seminar/workshop to review the SBRM process with sector security partners, especially Federal and private sector partners. Review existing risk/vulnerability assessment methodologies (asset/facility level, system level, and regional level) and possible future improvements.	NLT 90 days after SSP submission	SSAs
Convene joint GCC/SCC (Federal, private sector, and other entities) meeting to discuss development of SROs.	NLT 90 days after SSP submission	SSAs
Work with the DHS IP and Office of State and Local Government Coordination and Preparedness to engage State and local Homeland Security Advisors and other security representatives to determine long-range protective programs and initiatives.	NLT 90 days after SSP submission	SSA
Establish Transportation Systems SCC.	NLT 90 days after Transportation Systems SSP submission	Modal SCCs
Expand Research and Development Working Group (R&DWG) to include private sector R&D/technology community. Establish a regular schedule of joint government/industry meetings to continue overall outreach through briefings and conference participation to all transportation stakeholders and modes for reviewing existing R&D efforts and comparing results to R&D roadmaps and study recommendations.	NLT 90 days after SSP submission	SSA
Work with the Transportation Systems Sector GCC and SCC to develop sector CI/KR annual report.	July 1, 2007	SSAs

Milestone	Date	Lead Responsibility
Establish SROs that identify systems-based risk priorities.	NLT 180 days after SSP submission	GCC/SCC
Update and refine the DHS Top 100 list based on the SBRM process.	NLT 180 days after SSP submission	SSAs
Organize CIPAC joint Transportation Systems Sector task force composed of GCC and SCC members to address data collection—verifying data, risk assessment methods, how data may be collected, shared and possible approaches to collect information and data during transportation emergencies using published PCII rules.	NLT 180 days after SSP submission; ongoing	GCC/SCC
Establish Measurement Joint Working Group with sector security partners under the Transportation Systems Sector GCC and SCC.	NLT 180 days after SSP submission	SSAs
Establish Measurement Joint Response and Recovery Group with sector security partners under the Transportation Systems Sector GCC and SCC.	NLT 180 days after SSP submission	SSA
Consider establishing Joint Intel Working Group with sector security partners under the Transportation Systems Sector GCC and SCC.	NLT 180 days after SSP submission	SSA
Establish the R&D data-gathering approach, analysis, and distribution process with joint GCC/SCC agreement to include pending surface transportation security improvements (Federal, State, local, tribal, private, and academia).	NLT 180 days after SSP submission	SSA
Establish and make available lists of available technologies and products related to the protection of surface transportation to Federal, State, local, and tribal governmental entities and to private sector owners and operators of surface transportation systems.	NLT 180 days after SSP submission	SSA
Determine product and technology needs to inform the requirements for and prioritization of RDT&E.	NLT 180 days after SSP submission	GCC/SCC
Produce classified and non-classified threat assessments by mode.	NLT 180 days after SSP submission	SSA
Develop a regional approach for a public outreach conference(s) to address R&D transportation efforts.	NLT 270 days after SSP submission	SSA
Update NADB transportation taxonomy and attributes to reflect a systems view of the transportation network.	NLT 360 days after SSP submission	SSAs
Define sector-specific performance measures.	NLT 360 days after SSP submission	SSAs

6.6 Challenges and Continuous Improvement

TSA and its fellow stakeholders are using a metrics-based system of performance evaluation to provide a basis for documenting actual performance, facilitating systematic analysis, and promoting effective management. Metrics supply the data to affirm that specific goals are being met or to show what corrective actions may be required to stay on target.

The Transportation Systems Sector GCC and SCC will develop procedures to govern sector communication. The procedures will be consistent with continuous improvement models and will include frequency guidelines.

Sector Information Communication. A structured and focused communications strategy with the sector stakeholders will foster up-to-date knowledge of the best security plans, procedures, and programs. This will contribute to greater preparedness and resilience of transportation operations. TSA, working through the GCC, SCC, ISACs, State and local Fusion Centers, and other stakeholder associations and organizations, will disseminate areas for improvement, best practices, and lessons learned. Sector partners also will work to design and implement a communications strategy that will share information through the HSIN, Lessons Learned Information Sharing (LLIS), and other Web-based networks, as well as through modal forums (e.g., SCC/GCC), subject matter expert briefings, and special events, as needed. These efforts will provide a venue for stakeholder feedback on current security SSP and program effectiveness, successes, and areas of improvement, and the efforts will suggest future areas where stakeholders would recommend development, measurement options, and R&D activities.

Transportation Systems Sector GCC and SCC Decisionmaking. Milestones will be developed to monitor the SSP and program implementation progress. In addition, performance will be reviewed and tracked year after year to measure progress toward sector goals and the status of the sector's countermeasure programs. This periodic analysis will be used to focus the sector's attention on SSA strategies that require adjustment and protective programs that warrant programmatic changes, additional resources, or redirection. As a data baseline accumulates, expert opinion may be used to establish targets and associated milestones.

Measurement Challenges. There are many technical challenges facing the measurement program and the use of measurement data. The perceived largest challenges are effectively facilitating security partner's participation, effectively managing program costs and resources, developing and improving risk-reduction measurement techniques, gathering appropriate risk baseline data, enhancing cyber expertise, ensuring quality security measurements, and effectively sharing data.

7. Research and Development: CI/KR Protection

7.1 Overview of Transportation Systems Sector R&D

The Transportation Systems Sector recognizes the importance of working in concert with the NIPP and HSPD-7. The directive calls for the Secretary of Homeland Security to establish a comprehensive, integrated National Plan for CI/KR Protection and "[i]n coordination with the Director of the Office of Science and Technology Policy, the Secretary shall prepare, on an annual basis, a Federal Research and Development Plan in support of this directive."

The National Critical Infrastructure Protection Research and Development Plan (NCIP R&D Plan)[155] was developed as a result of HSPD-7 and it established a baseline for R&D capabilities required across all sectors. Prepared by the DHS S&T and the Office of Science and Technology Policy (OSTP), the NCIP R&D Plan highlights the R&D needs as having three primary "technology-enabling" goals and nine technology-centric themes.[156]

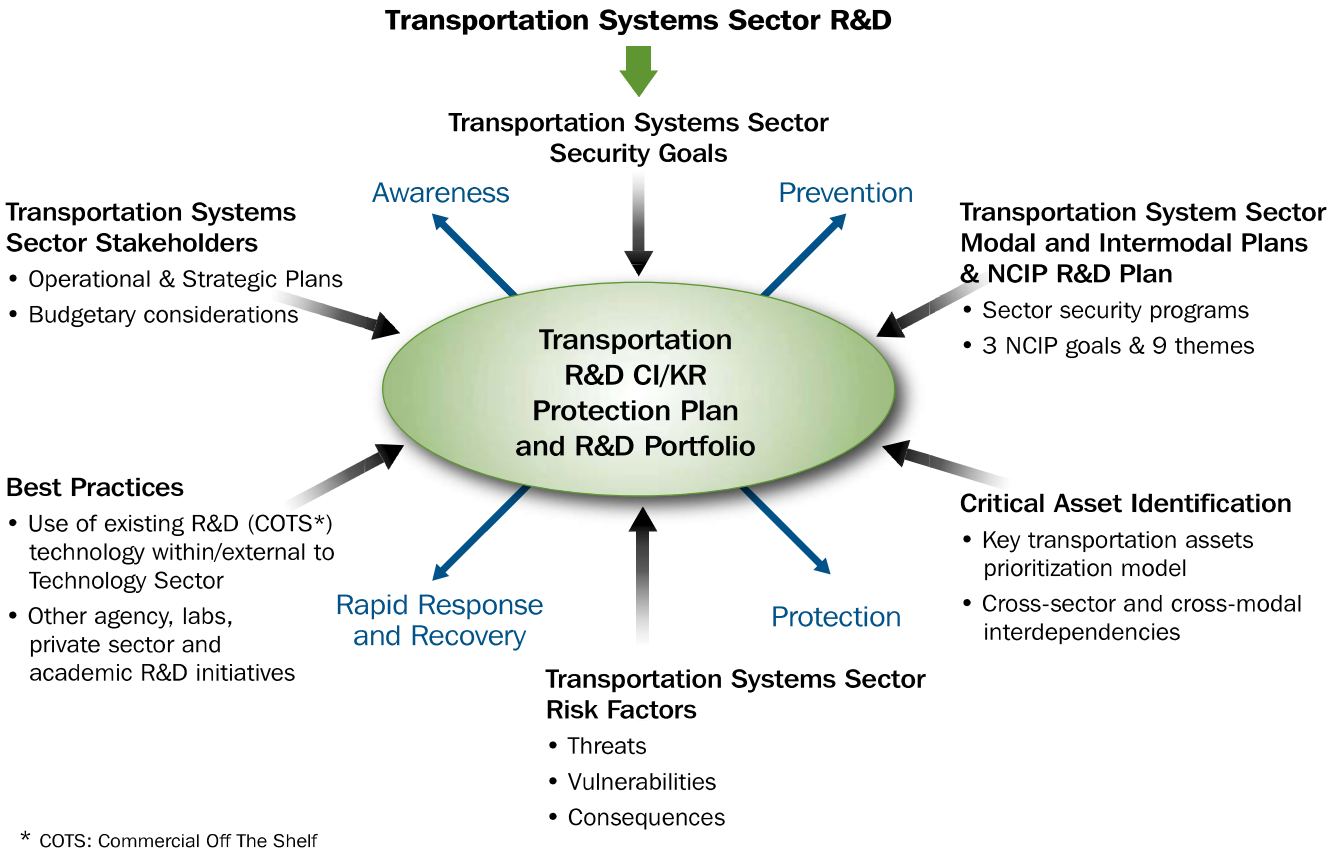
The Transportation Systems Sector's security goals support the overarching NIPP goal of a safer, more secure America and the prioritization of R&D investments. The strategic goals of the Transportation Systems SSP, together with the NCIP R&D Plan and the operational support needs of the government and private sector, provide the foundation for the sector CI/KR R&D Plan.

Figure 7-1 illustrates influencing factors in developing the R&D Plan.

[155] The NCIP Plan can be found on the DHS Web site at www.dhs.gov/xlibrary/assets/ST_2004_NCIP_RD_PlanFINALApr05.pdf.

[156] The three NCIP R&D technology enabling goals: (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; (3) resilient, self-diagnosing, and self-healing physical and cyber infrastructure systems. The nine technology-centric themes include: (1) detection and sensor; (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.

Figure 7-1: Transportation Systems SSP R&D Plan Influencing Factors



7.1.1 Transportation Systems Sector R&D Landscape

R&D has always been essential to the Transportation Systems Sector and represents a primary strategy to deter and prevent terrorist actions. Ongoing challenges to sector R&D efforts include the diversity of ownership of Transportation Systems Sector assets, inherent vulnerability of surface transportation, constant evolution of transportation security, and the increasing dependency on intermodal and international transportation. For these reasons, continual involvement by the private sector and other Transportation Systems Sector stakeholders is paramount to successfully address these challenges.

Transportation Asset Ownership Impact on R&D. A unique diversity of asset ownership and resultant accountabilities is found in the Transportation Systems Sector, with a large percentage of transportation systems and assets controlled by the private sector, as discussed in section 1. Such diversity of ownership calls for proactive and full engagement with all transportation security partners—Federal agencies; State, local, and tribal authorities; private sector businesses; trade organizations; and other transportation stakeholders—in order to expedite the flow of information and appropriately leverage R&D initiatives throughout the transportation community.

The diversity of the Transportation Systems Sector translates to a wide variety of security and risk management needs that depend on R&D efforts. Table 7-1 provides examples of such needs tied to specific infrastructure elements.

Table 7-1: Sample 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, 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 baggage and carry-on baggage to protect against weapons, explosives, 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 that stand alone to protect against weapons, explosives, 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.

The combination of diversity of ownership and wide dispersal of transportation system and asset needs creates a substantial challenge in coordination and planning that must be considered and included in the requirements for transportation R&D programs. Weaving security seamlessly into the fabric of the U.S. transportation network requires closely coupling and integrating R&D advances with security programs. Programs developed must be cost-effective, practical, and able to be integrated into a wide range of operational environments.

For these reasons, the Transportation Systems Sector R&D community must focus on advances in technology that impact practical integration issues at the operational level for achieving security goals while still emphasizing leap-ahead "game-changing" advances through basic (long-term) research.

Inherent Vulnerability of Surface Transportation. The very nature of surface transportation design and operations makes them vulnerable to attack. Surface transportation systems are far more accessible than the commercial passenger aviation system, with multiple entry points, few barriers to access, and with hubs that serve and allow transfers among multiple modes—intercity rail, commuter rail, subway, and bus—and multiple carriers.

Transportation Systems Sector R&D efforts must address the challenges of surface transportation security as laid out in Executive Order 13416, Strengthening Surface Transportation Security. Security technology developed for other purposes must be adapted to the different environment and circumstances of surface transportation. New technologies that are uniquely suited to mass transit and rail systems must be identified and developed.

Constant Evolution of Transportation Security. One of the primary characteristics of the transportation security environment is constant evolution. The terrorist threat poses special challenges since terrorists are highly adaptive—seeking to learn and

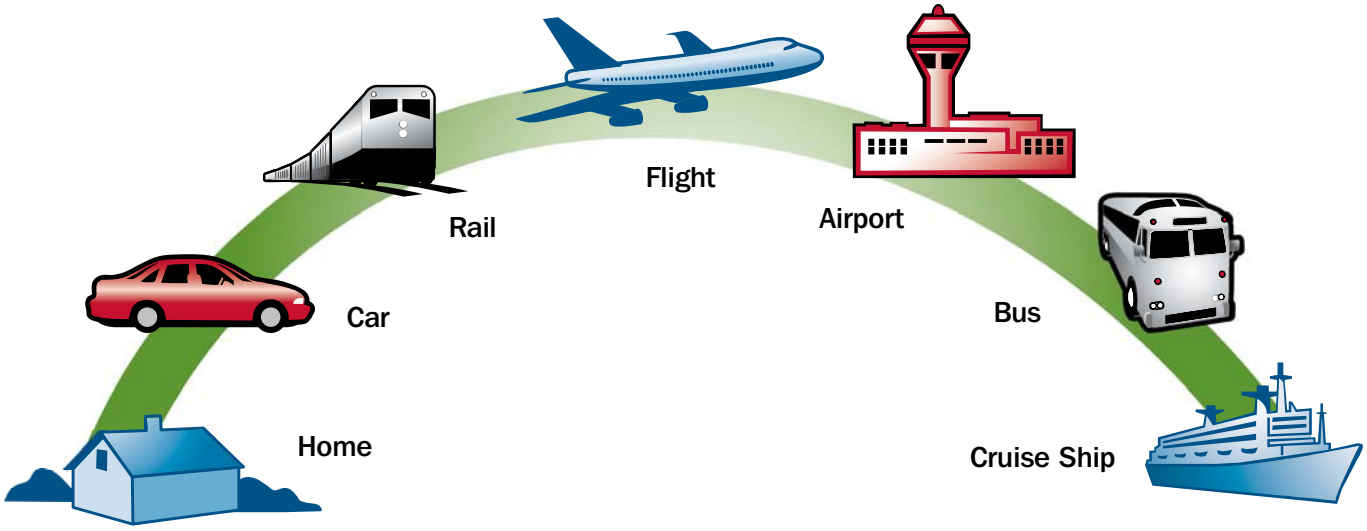
adjust their strategies based on past responses. Terrorists look for ways to defeat or get around current security measures by adapting to changes in security measures.

If a measure of unpredictability is built into operations, terrorists cannot use consistency to their advantage in planning an attack. Security approaches, therefore, must be based on flexibility and unpredictability.

Increasing Dependency on Intermodal Transportation. Driven by the increased mobility of today's society and the expansion of commerce domestically and globally, holistic intermodal security planning across all transportation modes is required. First, similar R&D efforts need to be leveraged across modes. Second, travel or commerce transactions, which span multiple transportation system modes, need analysis, coupled with comprehensive R&D programs, to minimize security exposures during handoffs between transportation modes.

Figure 7-2 illustrates an intermodal passenger transportation example.

Figure 7-2: Intermodal Passenger Transportation Example



International Considerations. The growth in shipment volumes into the United States from foreign ports and borders calls for R&D to solve multiple challenges in such a way that impediments to international commerce are minimized, while safety and security measures are maintained.

The development and implementation of common approaches to CIP and response to cross-border and transnational terrorist incidents is important to the security of America. 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.

Adjustments to supply chain controls and processes for enhanced cargo flow are in progress. These adjustments include using Known Shipper programs for commercial entities and designated foreign freight companies cleared under the DoD National Industrial Security Program. Developing the use of intelligent targeting systems to identify high-risk cargo and freight and enhanced inspection processes (e.g., using enhanced cargo scanning or an Explosive Detection System (EDS) and Radiation Portal Monitor (RPM)) will address enhanced security initiatives in anticipation of the continually rapid growth of imports into the United States.

7.1.2 Transportation Systems Sector R&D and Technology Community

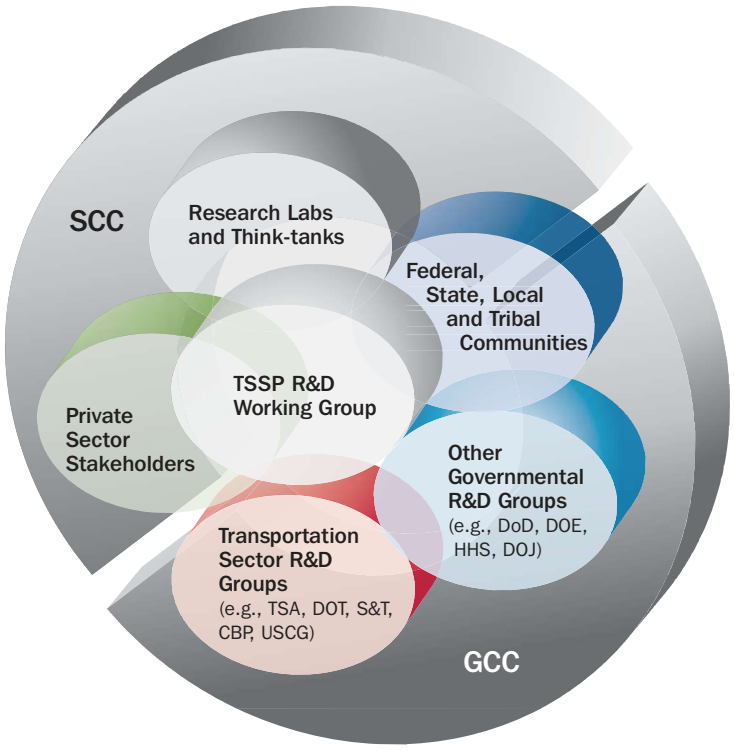
The sector stakeholders contributing to the R&D plan include:

- TSA;
- DHS S&T;
- Other DHS agencies, including USCG, CBP, and G&T;
- Sector-specific agencies, including DOT;
- Other Federal departments and agencies, including OSTP, DOC, USACE, and DoD R&D teams;
- State, local, and tribal DOTs and R&D organizations;
- Private sector owners, operators, and research entities; and
- Academia, national laboratories, and other research centers, including international entities.

7.1.3 Transportation Systems SSP R&D Working Group

Sector-specific planning and coordination are addressed through the GCC and SCC framework. A Transportation Systems SSP Research and Development Working Group (R&DWG) is formulated under these coordinating councils. The group is composed of representatives from the R&D community who are able to articulate long-range vision and requirements for the represented entity, who understand R&D technology capabilities and the inherent value of their potential ability to support that vision, and who have direct influence over the development of requirements and the use of technology within their entity or transportation mode. Figure 7-3 illustrates the Transportation Systems SSP R&DWG.

Figure 7-3: Transportation Systems SSP R&D Working Group



The role of the Transportation Systems SSP R&DWG is to coordinate and review R&D activities that directly or tangentially affect technologies that support the mission of the NCIP program. The primary mission of the Transportation Systems SSP R&DWG is to improve coordination and prioritization of sector RDT&E efforts and to leverage R&D programs across the stakeholder community.

The Transportation Systems SSP R&DWG will review R&D efforts in place across the Transportation Systems Sector and leverage existing initiatives to strengthen R&D efforts and jointly develop a Transportation Systems Sector R&D Plan. Fostering collaboration and encouraging knowledge sharing will facilitate talent and resource sharing, as will using best practices approaches through lessons learned.

The Transportation Systems SSP R&DWG will use the Transportation Systems Sector GCC and SCC to review the plans and recommendations made on behalf of the R&D transportation communities and may request specific actions from these groups to remove inhibitors in addressing CI/KR challenges. Special focus will be applied to cross-modal transportation challenges where process, policy, and use of technology intersect. Section 7.4, Transportation Systems Sector R&D Management Process, provides an expanded description of the Transportation Systems SSP R&DWG.

The initial tasks of the Transportation Systems SSP R&DWG listed below are further discussed in section 7.4.1:

- Assimilation of current R&D initiatives;
- Advancing the strategic way forward;
- R&D portfolio assessment; and
- Support for Executive Order 13416, Strengthening Surface Transportation Security.

7.1.4 R&D Alignment With Transportation Systems Sector Goals

Drawing from the Transportation Systems Sector goals and the technology-enabling vision of the NCIP R&D Plan, the Transportation Systems Sector R&D Plan will focus on the following strategic objectives:

Table 7-2: Alignment of Sector Goals and R&D Objectives

Transportation Systems Sector Goals	R&D Aligned Strategic Objectives
Prevent and deter acts of terrorism	Develop and deploy state-of-the-art, high-performance, affordable systems to prevent, detect, and mitigate the consequences of CBRNE attacks. 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 more frequent information sharing.
Enhance resilience of the U.S. transportation system	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). Architect dynamic, self-learning transportation network systems with tightly defined permissions for secure data access within a common operating picture. Develop layered, adaptive, secure nationwide enterprise architectures to facilitate shared situational awareness to enable real-time alerts to threats at an operational level. Develop equipment, protocols, and training procedures for response to and recovery from CBRNE attacks. Develop methods and capabilities to test and assess threats and vulnerabilities, prevent surprise technology, and anticipate emerging threats.
Improve the cost-effective use of resources	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. Align Transportation Systems 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 nomenclatures.

7.2 Transportation Systems Sector R&D Requirements

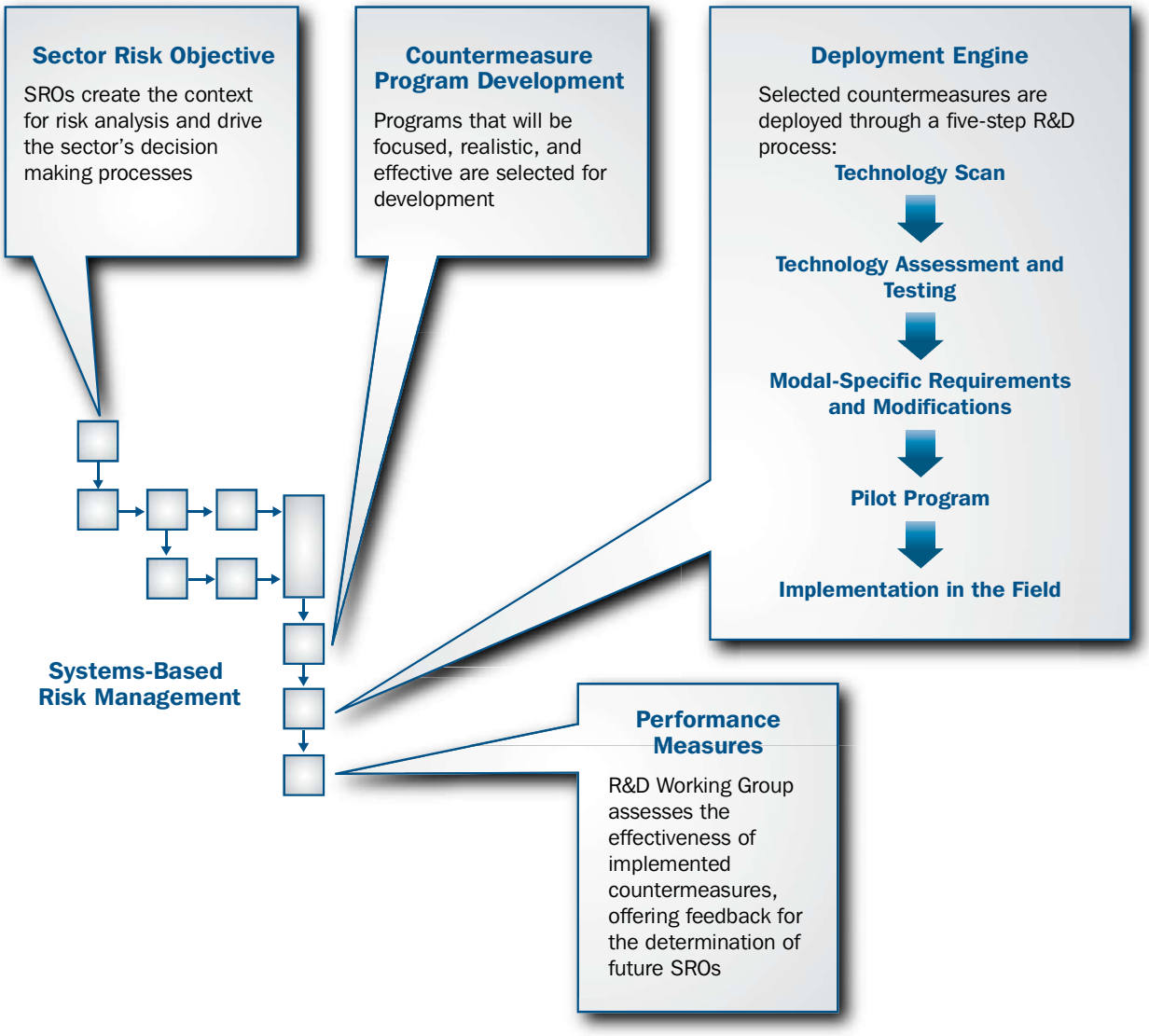
To achieve the Transportation Systems Sector security goals, certain essential capabilities must be obtained through effective R&D, such as:

- Improving existing technology to increase throughput, improve detection, lower false alarm rates, reduce staffing requirements, and improve operational effectiveness;
- Exploring emerging and revolutionary technology as additional security options to protect high-risk transportation assets;
- Developing efficient innovative technology solutions to prevent, protect, detect, respond, and recover;
- Developing security technology solutions to assist in event containment, mitigation of event consequences, and rapid response and recovery;
- Providing guidance on effectively integrating security technology solutions; and
- Creating computer models and algorithms that are interoperable to be accessible to critical infrastructure owners and operators. Also, use common inputs and assumptions.

7.2.1 Process for Defining Transportation Systems Sector Requirements

The risk-based process for identifying R&D requirements to develop these capabilities is illustrated in figure 7-4.

Figure 7-4: Sector-Wide R&D Risk-Driven Requirements Model



The SBRM framework described in sections 3, 4, and 5 will be used to identify and prioritize critical transportation systems and assets. Once the risks are identified, the areas of concern will be verified with appropriate government and stakeholder participants.

Risk mitigation options, including physical, process, and institutional changes, will be considered for these systems and assets. Assessing the options based on the alignment with sector security goals, NCIP R&D technology-enabling goals, and other guidance from sector stakeholders provides a prioritization of the mitigation options.

Under the leadership of TSA and the Transportation Systems Sector GCC and SCC partners, the Transportation Systems SSP R&DWG will enable collaboration across all stakeholders to identify the R&D-related capabilities that the sector currently has that could be used to mitigate any identified risks.

R&D efforts are derived using a technology-scan approach of available options to be considered, including current best practices. From these efforts, development programs are derived and often include identifying short-, medium-, and long-term desired outcomes. If approved, the path results in either a basic, applied, or development research program, or some combination thereof. These programs may then result in pilot test programs in the appropriate laboratories, followed by field testing and potential deployment.

Since Transportation Systems Sector R&D is a shared activity across the Federal Government and private sector, a great deal of insight is harnessed to help develop the appropriate technology requirements. Many of these requirements will be addressed through normal planning and programming activities.

Additional requirements that address intermodal transportation or exceed an individual stakeholder's ability to deliver must be collectively approached by the sector. Such requirements will be identified through the Transportation Systems SSP R&DWG outreach plans with other planning initiatives.

If the capability does not currently exist, the R&DWG will either take the lead in examining other programs that may be adapted to address the need or direct new R&D activities through the grants process or other funding vehicles to encourage new design capabilities.

R&D inputs to requirements are also driven by the evolution of technology capabilities. The continual scanning for new technology advances across the government, private sector, and academia enables greater potential deployment of technology-enabled solutions for enhanced security at the same or less cost than existing protection measures. It also reveals the potential for new security capabilities not previously considered.

7.2.2 Baseline Transportation Systems Sector Requirements

Examples of sector requirements derived from the SBRM process include:

1. **Enhance screening effectiveness for passengers, baggage, and cargo for all surface, maritime, and air transportation modes:**
   - 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 emerging and revolutionary technology to improve current screening and detect emerging threats.
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 to integrate into infrastructure and facilities;
   - Develop improved materials and methods to increase 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 security and homeland security purposes in a rapid, interoperable, and privacy-protective manner; and

– Recognize and expedite safe cargo entering 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 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.

7.2.3 Prioritization of Transportation Systems Sector R&D Requirements

Multiple criteria will be used to prioritize Transportation Systems Sector security requirements and assess the portfolio of new and existing initiatives. Consistent with OMB performance assessment tools and other best practices, the measures include:

- Relevance, such as correspondence with strategic goals, magnitude of strategic gap coverage, and level of risk mitigation;
- Compatibility with current operational environment;
- Cross-modal capability and potential;
- Quality of design;
- Performance, such as output and outcome measures, schedules, and decision points; and
- Time to complete or pilot-ready status.

New perspectives may be brought by the Transportation Systems SSP R&DWG to the course of an "in-development" program (e.g., insights on relevance, possible expansion or modifications, or other assistance).

7.3 Transportation Systems Sector R&D Plan

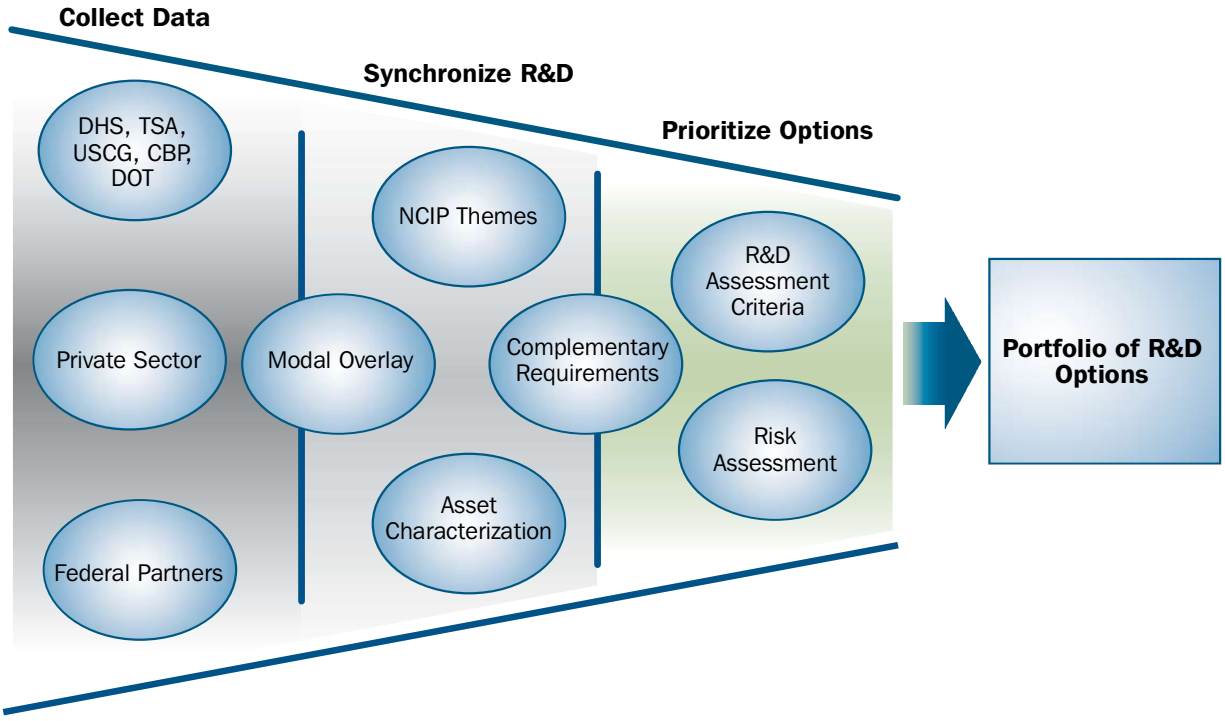
R&D in the Transportation Systems Sector will focus on advances in science and on the logical and practical integration issues at the operational and human performance level concurrently and rapidly, for achieving sector security goals. The mechanism for planning this integration and execution is the Transportation Systems Sector R&D Plan.

7.3.1 Components of the Transportation Systems Sector R&D Plan

The R&D Plan has two primary parts. The first part is reflective of the efforts undertaken by the sector to meet the sector goals. It describes the portfolio of existing initiatives that are designed to respond to specific requirements within the sector. This includes the Federal R&D community and R&D programs from the States and private industry related to the CIP. The second part of the plan takes a prospective view of the portfolio, focusing on new initiatives that meet the emerging and ongoing requirements of the sector.

Figure 7-5 illustrates the process for developing the R&D Plan.

Figure 7-5: Transportation Systems Sector R&D Plan Process



7.3.2 Sources of Input to the Transportation Systems Sector R&D Plan

To produce the Transportation Systems Sector R&D Plan, an initial review of transportation security R&D programs was conducted. Sources for this preliminary review included:

- TSA
- DOT
- CBP
- USCG
- OSTP
- DHS S&T
- National Science Foundation (NSF)
- DoD
- Other Federal R&D
- Miscellaneous sources

Plans are being developed to incorporate R&D programs from academia; the private sector; and other Federal, State, local, and tribal governmental entities to complete the data collection stage of the process.

7.3.3 R&D Portfolio Framework

A preliminary Transportation R&D Portfolio aggregates ongoing R&D efforts by the six individual modes of transportation: Aviation, Maritime, Mass Transit, Highway, Freight Rail, and Pipeline. One consolidated portfolio of programs relevant to intermodal transportation issues has been developed from the initial review of programs.

One of the more perplexing challenges is establishing a common baseline. Without common nomenclatures, definitions, or simple clarification of what is considered an R&D activity in one agency versus another, the ability to assimilate R&D initiatives for comparison purposes is potentially prone to misrepresentation. Once a common baseline is established, comparisons and groupings can be accumulated in a logical way.

A proposed matrix framework that maps the nine NCIP technology-centric R&D themes with a sector-specific asset categorization that recognizes the unique characteristics and requirements of transportation security will provide an advance toward developing a baseline for the Transportation Systems Sector R&D programs. This framework aligns the types of technology applicable to homeland security with the transportation system assets (infrastructures and components).

The NCIP R&D Plan is structured around themes that support all 17 critical infrastructure sectors. The nine themes were based on the repeated appearance in the concerns of infrastructure owners and operators, industry representatives, and government officials. Overlaying this theme-based structural model with people (passengers and employees), goods (baggage and cargo), conveyance, infrastructure, and facilities helps to create a logical framework from which to begin to assess the Transportation R&D Portfolio. The layered framework helps to identify complementary initiatives, duplications, and strategic gaps in existing and planned R&D efforts for the sector.

The framework will provide a common language and reference point that allows the comparison of R&D programs and will enable formulation of a strategic way forward. The framework does not attempt to dictate individual agency budget considerations or requirements.

Current Federal transportation security R&D initiatives have been mapped against the nine NCIP themes and associated subthemes as a first step toward developing the baseline R&D Portfolio. Particular emphasis was placed on identifying cross-modal programs for the sector.

The Transportation Systems SSP R&DWG will continue the process of assessing all stakeholders' current and planned R&D initiatives against the NCIP themes to assist in identifying research strategic gaps and requirements.

Once the data collection is completed and final framework charts are established and agreed upon, the Transportation Systems SSP R&DWG can develop summary conclusions about Transportation Systems Sector R&D programs, including:

- Strengths and goal coverage;
- Cross-modal capabilities and potentialities;
- Complementariness and interdependence of programs; and
- Opportunities for collaboration.

Completing the data collection and framework charts can help fulfill the requirements for Executive Order 13416, Strengthening Surface Transportation Security. This work will be conducted on an ongoing basis as part of the Transportation Systems SSP R&DWG activities.

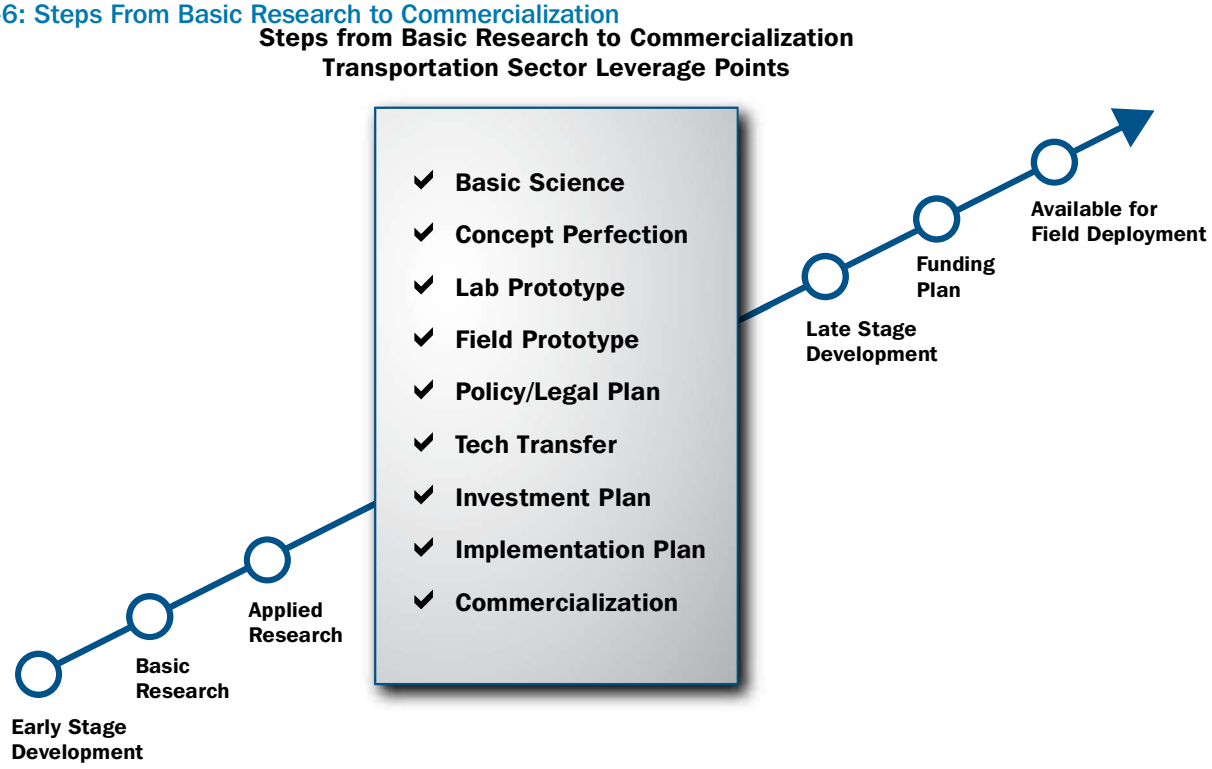
7.3.4 Technology Transition Through the R&D Life Cycle

All phases of research are required to bring potential technologies to bear for any given security challenge. The Transportation Systems Sector looks to the national laboratories and academia for basic research. The DHS S&T is utilizing the expertise of nine national laboratories under Section 309 of the Homeland Security Act of 2002 (Public Law 107-296). 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's University Transportation Centers (UTC), to direct funding of specific research programs, such as TSA-funded nanotechnology research at the University of North Carolina at Chapel Hill.

Applied research and early stage pilot test and development activities are the primary nature of transportation R&D activities by the transportation agencies and the private sector. 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 or private sector is necessary beyond this point to bring products to a commercially viable state.

The steps to bring to bear relevant technology capabilities into the field extend from the identification of basic research to eventual commercialization of a product. While each technology may require a different path to operationalization due to the uniqueness of the technology and the specific requirements of the transportation modes, a high-level process of leverage points within the R&D cycle for the Transportation Systems Sector is illustrated in figure 7-6.

Figure 7-6: Steps From Basic Research to Commercialization



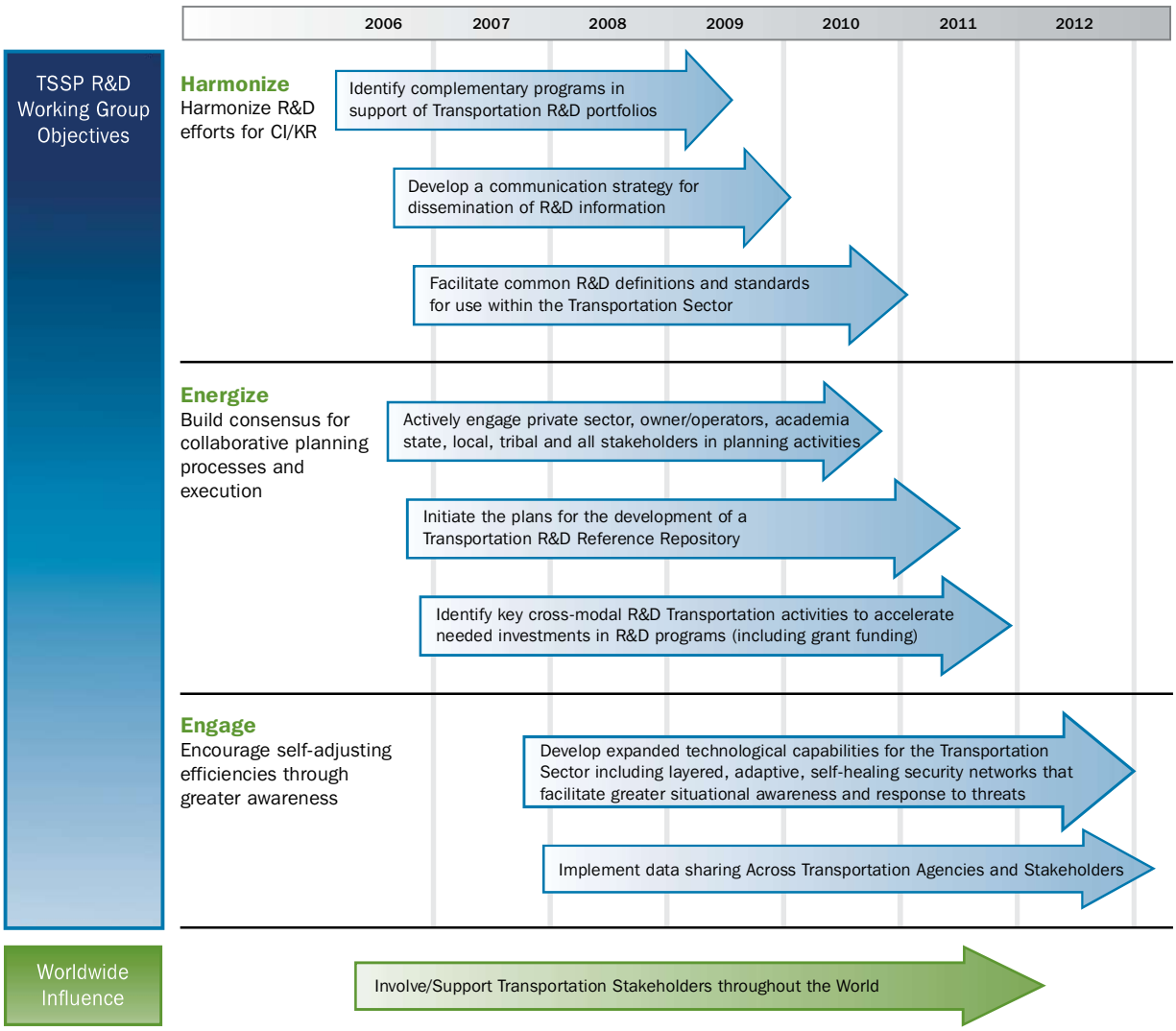
The Transportation Systems SSP R&DWG will work with the core governmental agencies, the DHS S&T, and private sector stakeholders to identify the appropriate process for leveraging common and cross-sector R&D initiatives to accelerate R&D developments where the greatest risks lie. As part of the portfolio development activities and identifying ways forward, the Transportation Systems SSP R&DWG, in partnership with private sector stakeholders and participating governmental agencies, will refine the development of more efficient processes to better leverage cross-organizational efforts, resources, and investments within the R&D and deployment cycles.

7.3.5 Transportation Systems Sector R&D Way Forward

Coordinating applied R&D initiatives across the transportation modes for increased security will require collaboration with the Federal, State, local, and tribal governments; the science community; the private sector; and the public at large. Eliminating Territorial boundaries of responsibility for achieving the greater purpose will take precedence in planning activities, whether governmental or private concerns. Understanding and accepting the risks, trade-offs, and priorities for increased security measures and contingency planning are the responsibility of all stakeholders in the Transportation Systems Sector.

Figure 7-7 highlights key planning objectives and milestones to be achieved in the next 5 years, including identifying technologies currently available to both government and private industry for immediate use. The creation of a technology clearinghouse, currently underway, is captured in the "Harmonize" section of the figure.

Figure 7-7: Transportation R&D Way Forward



7.4 Transportation Systems Sector R&D Management Process

7.4.1 Sector R&D Governance

The Transportation Systems SSP R&DWG is composed of members from core transportation stakeholders (see section 7.1.3) with the primary mission to improve coordination and prioritization of sector RDT&E efforts and to leverage R&D programs across the stakeholder community.

The strategic objectives of the R&DWG are to:

- Harmonize transportation R&D efforts for CI/KR 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 Transportation Systems SSP R&DWG will be supported by the Transportation Systems Sector GCC and SCC. The R&DWG will use these councils to review the plans and recommendations and, if needed, assist in removing inhibitors in addressing CI/KR challenges.

Membership is initially comprised of core government, national laboratories, and academic representatives, with the private sector engaged through the Transportation Systems SCC. Plans are being developed to fully integrate the private sector into the R&DWG.

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.

The initial tasks of the Transportation Systems SSP R&DWG in partnership with the broader transportation R&D communities include facilitation of the following.

Inventory and Assessment of Current R&D Initiatives

- Identify complementary technology requirements;
- Identify research strategic gaps;
- Publish non-confidential results of pilot tests within the Transportation Systems Sector;
- Identify cross-modal prioritization parameters; and
- Promote understanding of the use of infrastructure protection security grants to assist in implementing security requirements and guidelines for R&D transportation efforts.

Strategic Way Forward

- Actively engage private sector; academia; and State, local, and tribal agencies in planning activities;
- Facilitate and coordinate R&D planning activities across all sector modes; and
- Identify key cross-modal activities to accelerate investments in transportation R&D with a focus on risk-based needs.

R&D Portfolio Assessment

- Facilitate development of a common terminology and approach to characterize stages of R&D activities to improve technology transition; long- and short-term R&D requirements development for enhanced portfolio quality, including technology-scanning methods; and system vulnerabilities and transportation mode R&D priorities; and
- Develop and apply criteria to ensure that the current and planned R&D portfolio meets the future needs of the Transportation Systems Sector.

Support for Executive Order 13416, Strengthening Surface Transportation Security

- Maintain a list of current R&D initiatives that meet or have the potential to meet sector CI/KR protection challenges; and
- Facilitate the development of standards that meet transportation security CI/KR application needs, including surface transportation.

Future focus areas for the working group include:

- Coordinate community-level cross-sector and cross-agency proof-of-concept R&D pilot initiatives;
- Develop technology-scanning approaches to find and accelerate applicable security innovation from R&D within the private sector;
- Develop expanded technological capabilities that address intermodal and surface transportation challenges;
- Facilitate standards identification development;
- Coordinate communication strategy for dissemination of best practices, including development processes; and
- Establish community outreach to the transportation R&D community and transportation stakeholders.

The Transportation Systems SSP R&DWG will meet monthly to review portfolio characterization efforts and provide recommendations, inputs, and plans, including the annual update of the Transportation Systems SSP, and coordinate with the overall R&D programs in development with the varying stakeholders.

Within the Transportation Systems Sector, many R&D activities and entities have responsibility for cross-community coordination roles. Leadership engagement should be focused on optimizing the efforts of these entities for more effective and efficient R&D across the whole sector.

7.4.2 Coordination With Other Planning Efforts

The Transportation Systems SSP 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 and Executive Orders related to CI/KR, such as Executive Order 13416, Strengthening Surface Transportation Security, as they arise. The Transportation Systems SSP R&DWG will devise a set of principles and working methods for coordinating strategic planning activities among the contributing agencies and stakeholders.

The Transportation Systems SSP R&DWG will establish outreach plans with other planning initiatives. Examples of these are HSPD initiatives, the joint TSA and DOT Executive Steering Committee (ESC), and the Next Generation Airspace Transportation System's Joint Planning Development Office (NGATS/JPDO). Through the efforts of the Transportation Systems SSP R&DWG, the need for Transportation Systems Sector reporting will be aggregated, streamlining government and other similar reporting efforts required over time.

7.4.3 Importance of Private Sector Involvement

When fully established, the Transportation Systems SSP R&DWG will include the private sector and other nongovernmental group members involved in the Transportation Systems Sector or R&D community to collaborate in developing the Transportation Systems SSP R&DWG charter 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. There are numerous private industry entities that contribute to security research. For example, the freight rail industry conducts extensive research in the areas of safety, security, and efficiency at the Transportation Technology Center in Pueblo, Colorado. The goal of the R&DWG is to add private sector members to the team by first quarter of 2007.

The R&DWG is also establishing community outreach plans for State, local, tribal, and private sector entities to support more timely exchange of transportation security information. Improving the understanding of needs and requirements in the field by direct involvement and participation with local community efforts will improve the quality of R&D efforts and efficiencies. Future plans from these outreach efforts include reducing security risks by virtue of better coordination and identifying high-value potential pilot R&D programs that foster collaboration between local government and agencies and between the private sector and citizens.

Equally responsible, the private sector has a critical role in implementing transportation security initiatives because of its ownership of a significant percentage of transportation assets. The R&DWG recognizes that security initiatives developed by the government must be closely coupled with the operational goals and requirements of the private sector to be effective.

In addressing the rapid evolution of terrorist threats, including the potential of advanced weaponry in the hands of terrorists with clear intent to harm, the Transportation Systems Sector R&D community does not have the luxury of developing pure science removed from its context. Rather, in partnership with government and private sector teams, R&D initiatives can be quickly, safely, and cost-efficiently integrated into operational environments in parallel with game-changing research aimed at new and emerging threats. Keeping our communities safe under threat of attack will require community accountability and a heightened state of awareness between stakeholders and the transportation R&D community to effectively identify and mitigate risks and deter or respond to threats.

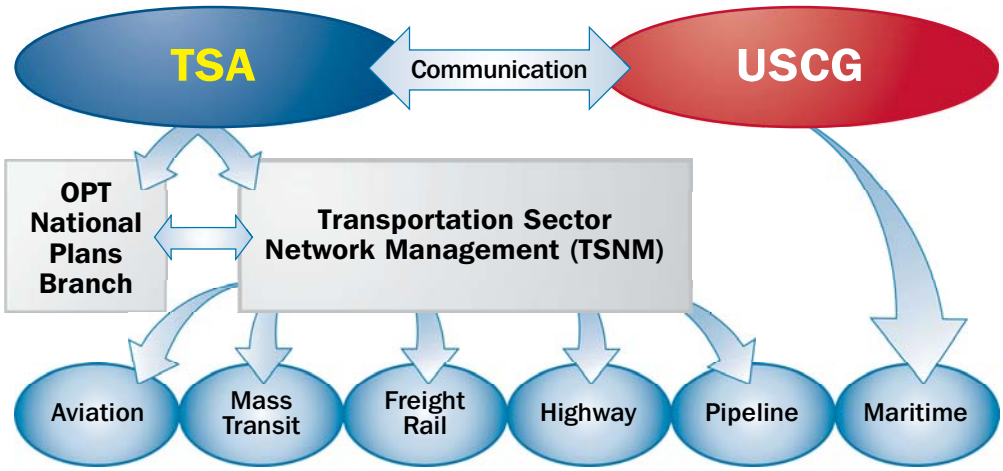
8. Manage and Coordinate SSA Responsibilities

This section describes the management process for supporting all NIPP-related responsibilities and how these responsibilities will be achieved. Additionally, this section outlines the NIPP information-sharing mechanisms that the Transportation Systems Sector uses, and details the processes, programs, and tools in place to ensure protection of the CI/KR information collected.

8.1 Program Management Approach

TSA, as the Transportation Systems Sector SSA, created a National Plans Coordination Branch, a new division under the Office of Operational Process and Technology (OPT), RMSP Division. The primary responsibility of the division is to align national strategic planning efforts such as the NIPP. Through this division, all TSA SSA responsibilities outlined in the NIPP will be performed and executed. The SSA is also responsible for the program management function of developing, updating, and implementing the Transportation Systems SSP in coordination with all security partners through the GCC/SCC framework. This approach is further depicted in figure 8-1. The USCG, as the SSA for the maritime transportation mode and as the chair of the Maritime Modal GCC, will continue to work cooperatively and collaboratively with the TSA; CBP; and other Federal, State, local, and tribal agencies. The Maritime Modal GCC will work with industry security partners to implement the NIPP requirements of CI/KR protection—to help prevent, prepare for, protect against, respond to, and recover from terrorist attacks, natural disasters, and other emergencies.[157] TSA also has responsibilities for coordinating and executing sector security strategies.

Figure 8-1: Transportation Sector Network Management Structure



[157] The NIPP and the NRP together provide a comprehensive, integrated approach to the homeland security mission (NIPP, June 2006, p. 6).

8.1.1 Transportation Sector Network Management

Based on the Secretary of Homeland Security's Second Stage Review (2SR) initiative and the vision TSA leadership holds, TSA adopted an organizational structure arranged along mode-specific lines. Each modal GCC, chaired by a Transportation Sector Network Management (TSNM) general manager, will focus on implementing transportation security planning efforts and coordinating key industry and stakeholder functions, such as modal implementation plans. The benefits of this structure are:

- Effective communication and coordination with industry stakeholder entities to collaboratively address security needs important to the sector, such as sharing robust risk, intelligence, and threat information;
- A coordinated and focused approach for addressing private sector security initiatives and activities through the NIPP SPM that will lead to effective policy and security decisions for all modes of transportation; and
- Enhanced information-sharing protocols through the GCC and SCC and other mechanisms to ensure timely and data-driven planning and decisionmaking.

Using the GCC/SCC structure, the SSAs will work with transportation security partners to ensure that effective program management and communications tools are in place to accomplish the future milestones described in section 6.

8.2 Processes and Responsibilities

8.2.1 SSP Maintenance and Update

The Transportation Systems SSP is an evolving document and, as such, it needs to be maintained and updated based on significant events, changes in the sector's security posture, or changes to the sector's approach to securing the sector. Because the Transportation Systems Sector is inherently complex in organizing around CI/KR protection efforts, the Transportation Systems SSP is a 3- to 5-year strategic planning document collaboratively developed using the GCC/SCC framework. Since the May 2007 version of the Transportation Systems SSP will be the sector's initial step in delineating a revised approach to augmenting the sector's CI/KR protection efforts, the Transportation Systems SSP will undergo periodic updates. This process can align with the NIPP triennial update cycle once the sector's leadership framework (Transportation Systems Sector GCC and Transportation Systems SCC) determines that the Transportation Systems SSP fully reflects and encompasses the sector's refinements in an SBRM approach; aligns resources to targeted programs and initiatives; measures the effectiveness of security programs, actions, and initiatives; and establishes a sector-wide R&D and information-sharing approach.

8.2.2 Resources and Budgets

As the SSAs, TSA and USCG, working with the GCC/SCC framework, will outline their respective CI/KR protective requirements and related budgeting information as part of the OMB/Federal budgeting process outlined in the NIPP through the sector CI/KR Protection Annual Report. TSA will initiate appropriate information-gathering efforts with all security partners during the February-to-June timeframe of each fiscal year to assist in the preparation of the annual report. The process for determining important and relevant CI/KR programs will include appropriate consideration of information provided by the transportation security partners, based on SROs, cost-effectiveness, and value to the overall sector's security needs. This sector-wide analysis will inform and facilitate determinations regarding which security programs merit consideration to target for funding through the OMB budgeting cycle.

Additionally, the USCG, as the SSA for the Maritime Mode, will work within its own budget models to provide justifications and execution plans for its security programs. As a multi-mission service, the USCG's assets are used to meet requirements from across its 11 federally mandated mission programs, one or more of which may contribute to CI/KR protection. The USCG

does not have a program dedicated to CI/KR protection, but is able to extrapolate and infer degrees of effort that contribute to infrastructure protection, and will use such methods in its approach to CI/KR risk management.

As previously mentioned, the sector-wide analysis is in no way intended to remove the budgetary discretion of individual agencies in submitting budget requests. Among agencies across the sector, determinations on which security programs merit consideration for additional funding shall be advisory only in nature.

8.2.3 Training and Education

The Transportation Systems SSP SBRM framework cannot be accomplished without robust training and continuous education to expand and augment organizational and individual CI/KR protection expertise.

Transportation Systems Sector security partners would greatly benefit from continued training and education on many security-related areas, such as risk evaluation and assessments, response and recovery, and other CI/KR security-related topics. An example course is the CI/KR Protection Qualification Course/Curriculum for Federal employees. The course will be available to all Federal employees whose CI/KR job performance involves at least 50 percent of their duties in analysis or assessment. This certified baseline training course offers agencies a standard for assessing CI/KR. To attend the course, students are required to complete a list of prerequisites and submit online learning certificates of completion. The course outline includes, among other topics:

- NIPP and CIP Overview;
- Risk Management Concept;
- Cyber, Physical, and National Security;
- Operations Security (OPSEC);
- Interdependencies (three key infrastructure interdependencies: water, electric, and power); and
- Grants Process (BZPP).

8.3 Implementing the Sector Partnership Model

As described in section 1 and further addressed in the modal implementation plans, the NIPP SPM is strongly advocated throughout the Transportation Systems SSP and the modal implementation plans as a collaborative mechanism for government and private industry to work together in protecting the Nation's critical infrastructure. Through this collaborative framework, both government and private industry security partners will facilitate cross-cutting planning, policy setting, coordination, and information sharing to determine the most cost-effective, efficient, and targeted approach for developing and implementing security programs based on a risk management framework.

8.3.1 Coordinating Structures

The Transportation Systems Sector established its GCC in January 2006. Since the sector functions by mode, the Transportation Systems Sector GCC is further segmented and organized by modal GCCs (Aviation, Maritime, Mass Transit, Highway, Freight Rail, and Pipeline), as well as by modal SCCs. The primary objective of the Transportation Systems Sector GCC and the forthcoming Transportation Systems SCC is to provide effective coordination for transportation strategies, initiatives, policies, and information sharing between the Federal Government, private industry, sector, and other security partners. The modal implementation plans are separate annexes to the Transportation Systems SSP, allowing modal GCCs and SCCs to develop specific plans to address how each mode will achieve the sector goals.

8.4 Information Sharing and Protection

As described earlier in this plan and detailed further in the modal implementation plans, a necessary component of the SPM is information sharing. The sharing of important and relevant security information between Federal, State, local, and tribal governments must occur frequently. While the sector's GCC/SCC framework is an effective way for government and private sector representatives to communicate and coordinate efforts, additional mechanisms are available that foster good communication and information sharing. The DHS has established several information-sharing platforms to disseminate and receive information.

Homeland Security Information Network. HSIN is a highly secure network backbone built over the Internet with a common set of information-sharing functions and tools for various private sector communities with common security interests. This network, in particular the portal for CIP called Critical Sectors (HSIN-CS), is a suite of tools that sector councils can use for information sharing, coordination, and communication about alerts, incidents, and planning efforts within the sector. This supports the exchange of threat information to critical infrastructure owners and operators in a variety of industries and locations, first-responders, and local officials.

Information Sharing and Analysis Centers (ISACs). ISACs exist within the Transportation Systems Sector, including mass transit, surface transportation (freight rail), highway, and maritime. Sector councils are not intended to replace the information-sharing functions provided by the ISACs. For those sectors that had established ISACs prior to the development of the NIPP, the sectors may continue to rely on them for operational and tactical capabilities for information sharing, such as threat alerts, and, in some cases, support for incident response activities.

The information-sharing process within each mode is further described in the modal annexes.

To facilitate the mandates of the Aviation and Transportation Security Act (ATSA), TSA has operationally coordinated and worked with transportation industry ISACs daily. Various ISACs have access to and work with the Transportation Security Operations Center (TSOC) and with TSA's modal experts and intelligence personnel. ISAC personnel have access to information and intelligence consistent with security policies. Working with ISACs supports the following ATSA requirements:

- TSA receives, assesses, and distributes intelligence information related to transportation security;
- TSA assesses threats to transportation;
- TSA serves as the primary liaison for transportation security to the intelligence and law enforcement communities;
- TSA coordinates countermeasures with appropriate departments; and
- TSA manages and provides operational guidance to field security resources daily.

In addition, ATSA tasks TSA with data sharing, correlating and safeguarding data, and performing a cooperative analysis to identify and effectively respond to threats to transportation security. The goals of continued daily, operational ISAC coordination are to continue:

- Improving methods of receiving information from transportation and transportation-related industries through ISACs, as well as coordinating and sharing information and intelligence with the industry;
- Seeking transportation and transportation-related industry participation in ISACs;
- Meeting quarterly with intelligence analysts (ISAC analysts) to review threat level; and
- Providing transportation and transportation-related ISACs access to the TSOC and to appropriate information and intelligence related to the security of the transportation industries.

Homeport. Homeport is the USCG's newest tool for providing information and service to the public over the Internet. It is an enterprise Internet portal that combines secure information dissemination, advanced collaboration, and provides a public-facing interface for internal USCG processes. In its first release, Homeport supports secure information sharing. Homeport version 1.0 provides information dissemination and collaboration for Area Maritime Security Committees (AMSCs), as well as e-mail notification capabilities. The public can access information related to Marine Safety, Security, and Environmental Protection missions, including, but not limited to, regulations, policy, publications, and forms. Homeport version 1.0 supports several different types of end users, including the general public, vessel and facility security officers, USCG personnel, and maritime committee members.

Area Maritime Security Committees. USCG sponsors an AMSC for each USCG Captain of the Port zone. The AMSCs, under the direction of a Federal Maritime Security Coordinator (FMSC), are a cornerstone of U.S. national maritime security, coordinating and collaborating with various Federal, State, and local authorities and private sector maritime stakeholders toward enhancing and maintaining port security. The AMSCs have already played an integral role in developing the various Area Maritime Security Plans required under the Maritime Transportation Security Act (MTSA). Additionally, the AMSC provides advice on identifying critical port infrastructure and operations, determines mitigation strategies and implementation methods, develops and describes processes for continuous evaluations of overall port security, serves as a link for communicating threats and changes in Maritime Security (MARSEC) levels, and disseminates appropriate security information to port stakeholders.

Critical Infrastructure Warning Information Network. This private government network is within HSIN and provides mission-critical connectivity and a survivable DHS capability for information sharing, collaboration, and alerting Federal, State, and local agencies on critical infrastructure restoration when primary forms of communication to the agencies are unavailable.

Appendix 1: List of Acronyms and Abbreviations

AAR	Association of American Railroads
AASHTO	American Association of State Highway and Transportation Officials
ACAMS	Automated Critical Asset Management System
AFSD-LE	Assistant Federal Security Directors for Law Enforcement
AFSP	Alien Flight Student Program
AGA	American Gas Association
AIP	Airport Improvement Program
AIS	Automated Identification System
AMSC	Area Maritime Security Committee
AMSP	Area Maritime Security Plan
ANSI	American National Standards Institute
AOPA	Airport Operators and Pilots Association
AOPL	Association of Oil Pipe Lines
APEC	Asia-Pacific Economic Cooperation
APGA	American Public Gas Association
API	American Petroleum Institute
APTA	American Public Transportation Association
ASAC	Aviation Security Advisory Committee
ASC	Airport Security Coordinator
ASI	Aviation Security Inspector
ASME	American Society of Mechanical Engineers
ASP	Airport Security Program
ASTM	American Society for Testing and Materials
ATS	Automated Targeting System
ATSA	Aviation and Transportation Security Act
ATU	Amalgamated Transit Union
AWW	America's Waterway Watch
BART	Bay Area Rapid Transit
BASE	Baseline Assessment and Security Enhancement
BIS	Bureau of Industry and Security
BZPP	Buffer Zone Protection Program
CARVER	Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability.
CBP	Customs and Border Protection
CBRNE	Chemical, Biological, Radiological, Nuclear, and (High-Yield) Explosive
CCTV	Closed-Circuit Television
CD	Compact Disc
CDL	Commercial Driver's License
CFR	Code of Federal Regulations
CI/KR	Critical Infrastructure and Key Resources
CIP	Critical Infrastructure Protection
CIPAC	Critical Infrastructure Partnership Advisory Council
CISO	Chief Information Security Officer
CMC	Crisis Management Center
COBIT	Control Objectives for Information and Related Technology

COOP	Continuity of Operations
CR	Comprehensive Reviews
CSI	Container Security Initiative
CSR	Corporate Security Review
CTA	Chicago Transit Authority
CTAA	Community Transportation Association of America
C-TPAT	Customs-Trade Partnership Against Terrorism
DART	Dallas Area Rapid Transit
DCA	Ronald Reagan Washington National Airport
DEA	Drug Enforcement Administration
DHHS	Department of Health and Human Services
DHS	Department of Homeland Security
DNDO	Domestic Nuclear Detection Office
DOC	Department of Commerce
DoD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
DOS	Department of State
DOT	Department of Transportation
DPA	Defense Production Act
DSS	Decision Support System
EAT	Engineering Assessment Team
ECAC	European Civil Aviation Conference
EDS	Explosives Detection System
EMS	Emergency Medical Services
ESC	Executive Steering Committee
EU	European Union
FAA	Federal Aviation Administration
FACA	Federal Advisory Committee Act
FAF	Freight Analysis Framework
FAM	Federal Air Marshal
FAMS	Federal Air Marshal Service
FAS	Freight Assessment System
FBI	Federal Bureau of Investigation
FBO	Fixed-Base Operator
FDA	Food and Drug Administration
FEMA	Federal Emergency Management Agency
FERC	Federal Energy Regulatory Commission
FHWA	Federal Highway Administration
FIG	Field Intelligence Group
FISMA	Federal Information Security Management Act
FIST	Field Intelligence Support Team
FLETC	Federal Law Enforcement Training Center
FMCSA	Federal Motor Carrier Safety Administration
FMSC	Federal Maritime Security Coordinator
FOUO	For Official Use Only
FPC	Federal Port Controller
FRA	Federal Railroad Administration
FRZ	Flight Restricted Zone
FSD	Federal Security Director
FSMP	Facility Security Management Program
FSR	Freight Security Requirement
FTA	Federal Transit Administration
FY	Fiscal Year
G8	Group of 8
G&T	Office of Grants and Training
GA	General Aviation
GA@DCA	Restoration of GA at Ronald Reagan Washington National Airport
GCC	Government Coordinating Council
GDP	Gross Domestic Product
GIS	Geographic Information Systems
GIWW	Gulf Intracoastal Waterway
GPRA	Government Performance and Results Act
GPS	Global Positioning System
GTI	Gas Technology Institute
HACCP	Hazardous Analysis and Critical Control Point
HAZMAT	Hazardous Materials

HITRAC	Homeland Infrastructure Threat Risk Analysis Center
HOT	Hidden and Obviously Typical
HSAS	Homeland Security Advisory System
HSC	Homeland Security Council
HSIN	Homeland Security Information Network
HSPD	Homeland Security Presidential Directive
HTUA	High Threat Urban Area
I&A	Office of Intelligence and Analysis
IAC	Indirect Air Carrier
ICAO	International Civil Aviation Organization
ICC	Intelligence Coordination Center
ICE	Immigration and Customs Enforcement
ICS	Incident Command System
IED	Improvised Explosive Device
IFR	Instrument Flight Rules
IIIS-D	Integrated Intermodal Information System Domestic
IMO	International Maritime Organization
INGAA	Interstate Natural Gas Association of America
IP	Office of Infrastructure Protection
IPMP	Integrated Protective Measures Plan
IPP	Infrastructure Protection Program
IPSLO	International Port Security Liaison Officer
ISAC	Information Sharing and Analysis Center
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
ISPS	International Ship and Port Facility Security
ISSO	Information System Security Officer
ISSP	Information Systems Security Program
IT	Information Technology
JPDO	Joint Planning and Development Office
JTTF	Joint Terrorism Task Force
JVA	Joint Vulnerability Assessment
LAN	Local Area Network
LES	Law Enforcement Sensitive
LLIS	Lessons Learned Information Sharing
LNG	Liquefied Natural Gas
LTATP	Land Transportation Anti-Terrorism Training Program
MANPAD	Man-Portable Air Defense System
MARAD	Maritime Administration
MARC	Maryland Rail Commuter
MARSEC	Maritime Security
MARTA	Metropolitan Atlanta Rapid Transit Authority
MAST	Maritime Analysis Support Tool
MBTA	Massachusetts Bay Transportation Authority
MDA	Maritime Domain Awareness
MIRP	Maritime Infrastructure Recovery Plan
MMCT	Multi-Modal Criticality Tool
MOU	Memorandum of Understanding
MSC	Maritime Security Committee
MSRAM	Maritime Security Risk Assessment Model
MSST	Maritime Safety and Security Team
MTS	Maritime Transportation System
MTSA	Maritime Transportation Security Act
MTSNAC	Marine Transportation System National Advisory Council
NADB	National Asset Database
NAS	National Airspace System
NCIP	National Critical Infrastructure Protection
NCSD	National Cyber Security Division
NCTC	National Counterterrorism Center
NEDCTP	National Explosives Detection Canine Team Program
NETL	National Energy Technology Laboratory
NextGen	Next Generation Air Transportation System
NGATS	Next Generation Air Transportation System
NICC	National Infrastructure Coordination Center
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan

NISAC	National Infrastructure Simulation and Analysis Center
NIST	National Institute of Standards and Technology
NMSAC	National Maritime Security Advisory Committee
NMTSP	National Maritime Transportation Security Plan
NOA	Notice of Arrival
NOAA	National Oceanic and Atmospheric Administration
NORAD	North American Aerospace Defense Command
NPIAS	National Plan of Integrated Airport Systems
NPRA	National Petrochemical and Refiners Association
NPRN	National Port Readiness Network
NRC	National Resource Center
NRP	National Response Plan
NSF	National Science Foundation
NSMS	National Strategy for Maritime Security
NSPD	National Security Presidential Directive
NSPI	National Strategy for Pandemic Influenza
NSSE	National Security Special Event
NSTS	National Strategy for Transportation Security
NTI	National Transit Institute
NTIA	National Telecommunications and Information Administration
NTS	National Transportation System
OCC	Operations Control Center
OI	Office of Intelligence
OMB	Office of Management and Budget
ONG	Oil and Natural Gas
ONI	Office of Naval Intelligence
OPT	Office of Operational Process and Technology
OSC	Operation Safe Commerce
OSTP	Office of Science and Technology Policy
PART	Performance Assessment and Rating Tool
PCII	Protected Critical Infrastructure Information
PHMSA	Pipeline and Hazardous Materials Safety Administration
PPBE	Planning, Programming, Budgeting, and Execution
PSGP	Port Security Grants Program
PSI	Principal Security Inspector
R&D	Research and Development
R&DWG	Research and Development Working Group
R&RWG	Response and Recovery Working Group
RAMCAP	Risk Analysis Methodology for Critical Asset Protection
RASM	Risk and Strategy Matrix
RDD	Radiological Dispersal Device
RDT&E	Research, Development, Test, and Evaluation
RFID	Radio Frequency Identification
RMD	Risk Management Division
RMSC	Regional Maritime Security Coalition
RMSP	Risk Management Strategic Planning
RPM	Radiation Portal Monitor
RSC	Rail Security Coordinator
RSP	Rail Security Pilot
S&T	Science and Technology Directorate
SAAP	Security Analysis and Action Program
SAFETEA-LU	Safe, Affordable, Flexible, Efficient Transportation Equity Act: A Legacy for Users
SAI	Security Action Item
SAV	Site Assistance Visit
SBRM	Systems-Based Risk Management
SBU	Sensitive But Unclassified
SCADA	Supervisory Control and Data Acquisition
SCC	Sector Coordinating Council
SCOTS	Special Committee on Transportation Security
SD	Security Directive
SIDA	Security Identification Display Area

SIPT Security Integrated Product Team

SLFC State and Local Fusion Center

SPM Sector Partnership Model

SPP Security and Prosperity Partnership of North America

SRO Strategic Risk Objective

SSA Sector-Specific Agency

SSD Systems Support Division

SSI Sensitive Security Information

SSOA State Safety Oversight Agency

SSP Sector-Specific Plan

SST Smart and Secure Trade Lanes

ST-ISAC Surface Transportation Information Sharing and Analysis Center

STSI Surface Transportation Security Inspection

T4 Transit Terrorist Tools and Tactics

TAPA Technology Asset Protection Association

TARR Terrorist Awareness Recognition and Reaction

TCLDR Transit, Commuter, and Long-Distance Rail

TFSSP Twelve-Five Standard Security Program

TIH Toxic Inhalation Hazard

TRAM Transit Risk Assessment Module

TRANSCAER Transportation Community Awareness and Emergency Response

TRB Transportation Research Board

TSA Transportation Security Administration

TSGP Transportation Security Grant Program

TSNM Transportation Sector Network Management

TSOC Transportation Security Operations Center

TSSD Transportation Security Situation Display

TVC Threats, Vulnerabilities, and Consequences

TWIC Transportation Worker Identification Credential

UASI Urban Area Security Initiative

USACE U.S. Army Corps of Engineers

US-CERT United States Computer Emergency Readiness Team

USCG U.S. Coast Guard

USDA U.S. Department of Agriculture

USFORSCOM U.S. Forces Command

USNORTHCOM U.S. Northern Command

USTRANSCOM U.S. Transportation Command

UTC University Transportation Center

VBIED Vehicle-Borne Improvised Explosive Device

VBST Vessel Boarding and Security Team

VIPR Visible Intermodal Prevention and Response

ViSAT Vulnerability Identification Self-Assessment Tool

VTS Vessel Traffic System

WAN Wide Area Network

WCO World Customs Organization

WMATA Washington Metropolitan Area Transit Authority

WMD Weapon of Mass Destruction

Appendix 2: Glossary of Key Terms

Some 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 of 2002, USA PATRIOT Act of 2001, the National Incident Management System, the National Response Plan, and the National Infrastructure Protection Plan.

Asset. An asset is any person, facility, material, information, or activity that has a positive value to the Transportation Systems Sector. The asset may have value to an adversary, as well as an owner, although the nature and magnitude of those values may differ. Assets may be categorized in many ways, including people, information, equipment, facilities, and activities or operations.

Consequence. The negative effect, or effects, that can be expected if an asset or system is damaged, destroyed, or disrupted.

Countermeasure. A countermeasure is an action intended to induce institutional, process, and physical changes that reduce risks to systems and assets. The countermeasure may address a vulnerability, threat, consequence, or overall system performance.

Critical Infrastructure. Assets, systems, and networks, whether physical or virtual, so vital to the United States that the incapacity or destruction of such assets, systems, or networks would have a debilitating impact on security, national economic security, public health or safety, or any combination of those matters.

Cyber Security. The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information contained therein to ensure confidentiality, integrity, and availability. Includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, public safety answering points, and September 11 communications and control systems.

Dependency. The one-directional reliance of an asset, system, network, or collection thereof, within or across sectors, on input, interaction, or other requirement from other sources in order to function properly.

Function. The service, process, capability, or operation performed by specific infrastructure assets, systems, or networks.

Government Coordinating Council (GCC). The council comprised of representatives across various levels of government (Federal, State, local, and tribal) as appropriate to the security and operational landscape of each individual sector. The GCC is the government counterpart to the Sector Coordinating Council (SCC) for each sector established to enable interagency coordination.

Impact. See consequence.

Interdependency. The multi- or bi-directional reliance of an asset, system, network, or collection thereof, within or across sectors, on input, interaction, or other requirement from other sources in order to function properly.

Key Resources. Publicly or privately controlled resources essential to the minimal operations of the economy and government.

Materiality. Materiality is a function of consequence and likelihood. Strategic risks have a very high materiality (i.e., very significant consequence and high likelihood), whereas traditional risks have low materiality (i.e., low consequence and/or low likelihood).

Mega-Node. The single point at which multiple modes intersect. In transportation systems, a mega-node is a place of potential failure or bottleneck, with the potential for wide-ranging disruptions and losses.

Mitigation. Activities designed to reduce or eliminate risks to persons or property or to lessen the actual or potential effects or consequences of an 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. Examples of mitigation measures include zoning and building codes, floodplain buyouts, analysis of hazard-related data, and educating the public.

Mode. A specific form or variety of something. In the context of transportation, there are six modes: aviation, maritime, mass transit, highway, freight rail, and pipeline.

Network. A group of assets or systems that share information or interact with each other in order to provide infrastructure services within or across sectors.

Node. A network intersection or junction (e.g., a subway station).

Resilience. The capability of an asset, system, or network to maintain its function during or to recover from a terrorist attack, natural disaster, or other incident.

Risk. A measure of potential harm that encompasses threat, vulnerability, and consequence. In the context of the Transportation Systems Sector-Specific Plan (SSP), risk is the expected magnitude of loss due to a terrorist attack, natural disaster, or other incident, along with the likelihood of such an event occurring and causing that loss within or utilizing the sector.

Risk Management. The process of selecting and implementing security countermeasures to achieve an acceptable level of risk at an acceptable cost.

Risk Views. Risk views describe types of systems in terms of mode, geography, function, and ownership. These four views capture multiple ways of addressing systems and allow for a robust assessment of the Transportation Systems Sector.

Sector. The logical collection of assets, systems, or networks that provide a common function to the economy, government, or society. The Transportation Systems Sector is one of 17 critical infrastructure and key resources (CI/KR) sectors.

Sector Coordinating Council. The private sector counterpart to the GCC, this council is a self-organized, self-run, and self-governed representative of the sector's key stakeholders.

Sector Partnership Model. The framework used to promote and facilitate sector and cross-sector planning, coordination, collaboration, and information sharing for CI/KR protection involving all levels of government and private sector entities.

Sector-Specific Agency (SSA). Federal departments and agencies identified in Homeland Security Presidential Directive 7 (HSPD-7) as responsible for CI/KR protection activities in specified CI/KR sectors. The sector-specific agency for transportation is the Transportation Security Administration (TSA).

Sector-Specific Plan (SSP). The augmenting plan that complements and extends the National Infrastructure Protection Plan (NIPP) Base Plan, detailing the application of the NIPP framework specific to each CI/KR sector. SSPs are developed by the SSAs in close collaboration with other security partners. This document is the SSP for the Transportation Systems Sector.

Security Partner. Federal, State, regional, Territorial, local, or tribal governmental entities; private sector owners and operators; and representative organizations, academic and professional entities, and certain not-for-profit private volunteer organizations that share in the responsibility for protecting the Nation's CI/KR.

Strategic Risk. Those risks that impact the entire Transportation Systems Sector, threatening disruption across multiple stakeholder communities. The consequences of strategic risks can cross multiple sectors and can have far-reaching, long-term effects on the national economy, natural environment, or public confidence. Strategic risks are those that breach the threshold of risks that stakeholders are reasonably expected to manage on their own and move into an area of risk management. Illustrative examples of strategic risks to the sector could include: disruption of a mega-node in the transportation system (large-scale impact on national economic security), use of a component of the transportation system as a weapon of mass destruction (terrorism event leading to loss of life and of public confidence), and release of a biological agent at a major rail transfer station or hub airport (terrorism event affecting national public health and safety).

Strategic Risk Objective (SRO). A measurable target that, when attained, contributes to the accomplishment of a strategic goal.

System. A collection of assets that comprises a dynamic, complex, and unified whole. A system maintains its existence and functions as a whole through the interaction of its parts.

Systems-Based Risk Management (SBRM). A risk management framework that helps define and clarify countermeasure programs aimed at a specific SRO, which will be integrated into the sector's strategic plan. SBRM is an important element of the sector's approach to determining its risk priorities, documenting them as SROs, determining approaches for achieving these objectives, and defining what success means for each of the SROs through performance measures. The SBRM process yields strategic countermeasures.

Threat. The intention and capability of an adversary to undertake actions that would be detrimental to CI/KR.

Transportation. Conveyance of passengers or goods. There are six modes of transportation: aviation, maritime, mass transit, highway, freight rail, and pipeline.

Transportation Security Incident. A security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area.

Vulnerability. A vulnerability is a characteristic or flaw that renders an asset or system susceptible to destruction, incapacitation, or exploitation.

Appendix 3: Transportation Systems Sector Assessment Tools and Methodologies

The Transportation Systems Sector and its partners in the homeland security community use a number of different tools and methodologies to assess threats, vulnerabilities, and consequences to assist the Nation's CI/KR owners and operators in assessing the risk to their infrastructures. The DHS is working closely with Federal, State, and local emergency responders; law enforcement; private sector associations; owners and operators; and other regional officials to use these tools, as well as to identify the requirements for developing new tools to assess the risks to critical transportation infrastructure.

The sector currently uses a number of tools to assess threats, vulnerabilities, and consequences, and calculate the risk to the transportation infrastructure. Stakeholders use many of these tools voluntarily, and the sector provides them to public and private owners and operators at no expense. Government assessors use some tools and methodologies specifically to enforce regulations or to provide free technical expertise and education in conducting a risk assessment effectively. Methodologies will continue to be appropriately vetted before the sanctioning of any transportation subsector. TSA will work with the DHS to find and leverage similarities between the different tool sets now in use as the sector organizes and adopts a system-wide risk assessment approach.

Although not all-inclusive, the following paragraphs briefly describe some of the analysis tools that TSA and its key Federal partners use to assess risk within the sector.

Analytical Risk Management

Tool: ARM
Agency: Originally developed by the CIA Center for Security Excellence
Type: Self-Assessment Tool
Tool Assesses: Risk

Analytical Risk Management methodology is based on the CIA Analytical Risk Management process. The process consists of six steps that result in the identification of risk associated with vulnerability and effective countermeasures that the leadership can apply to mitigate the risk. Each assessment requires a tailored approach for the specific sector being assessed. Every sector has differences processes, information, facilities, raw materials, end products, operating principles, and procedures that make it unique. The analytical risk management process is specifically tailored to each of these differences. Throughout the process, each step and function is documented to provide an audit trail of the security decisions that are made.

CARVER Target Analysis and Vulnerability Assessment Tool

Tool: CARVER
Agency: TSA, numerous other agencies and organizations
Type: Self-Assessment and Government-Conducted Analytic Methodology
Tool Assesses: Vulnerability and Consequence

The Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability (CARVER) methodology is widely used throughout the Transportation Systems Sector as an easily employable methodology for owner/operators and Federal assessors to assess vulnerabilities and consequences against different threat scenarios. Often used by U.S. Special Operations Forces to target enemy installations or facilities or by force protection specialists to assess vulnerabilities from an adversary's point of view, TSA currently uses CARVER to assess the vulnerabilities and criticality of processes within the rail sector. As these factors are considered, they receive a numerical value related to the attractiveness of attacking the target. After all of the elements of a particular site are assessed against these factors, the site with the highest sum of values will be the most attractive target within the limits of that particular threat scenario.

Comprehensive Reviews

Tool: Comprehensive Review Process
Agency: DHS; TSA and Transportation Stakeholders
Type: Government-Facilitated Risk Assessment Tool
Tool Assesses: Vulnerability, Consequence, and Risk (system level); Threat provided by TSA

DHS Comprehensive Reviews contribute to the security of our Nation's critical infrastructure by thoroughly evaluating each significant facility's security; comparatively analyzing risk across the sectors; coordinating with Federal, State, and local response and recovery officials; identifying potential enhancements to security that can be made; and identifying additional measures that may protect against and mitigate the effects of terrorist attacks should they occur. The reviews enable the most effective allocation of homeland security resources. The Transportation Systems Sector began applying this tool in June 2006.

The Comprehensive Review process requires significant participation from private sector owners and operators, as well as Federal, State, and local officials. The GCCs of various sectors undergoing reviews work in close cooperation with their corresponding SCCs to foster participation in the review process. The Comprehensive Review team meets before the site visit and reviews the consequence and vulnerability information that the facility owner/operator provides, as well as the various pre-existing security and emergency response plans.

Each Comprehensive Review uses a standard set of tools and templates to develop a comparable estimate of the facility's vulnerability to a variety of threats, the range of consequences related to the threats, and an evaluation of existing security and response. The process provides a vehicle for discussion with stakeholders on potential enhancements to security in and around the site. This framework assists in reducing vulnerabilities, implementing appropriate security measures, and mitigating the potential consequences of a successful attack. To conduct a Comprehensive Review, a number of tools can be used, including the Vulnerability Identification Self-Assessment Tool (ViSAT) and eventually Risk Analysis and Management for Critical Asset Protection (RAMCAP).

After performing its site assessments, the Comprehensive Review team analyzes the information gathered and develops reports in both classified and For Official Use Only versions. The information is shared with appropriate stakeholders, including Federal agencies, State and local law enforcement, emergency management, and the facility owner/operators. Some outputs created from this process include:

- The site-specific Integrated Protective Measures Plan (IPMP) that identifies shortfalls in resources, evaluates response capabilities, and coordinates all agency-specific response plans, as well as training needs and options to address security and response challenges;
- The planning, tracking, and measurement of security and response enhancements in addition to the impact they have on the security and risk standing of the site; and
- Standardized risk data to enable a cross-sector comparative risk assessment, and investment and budgeting decisions.

Constellation/Automated Critical Asset Management System (ACAMS)

Tool: Constellation/ACAMS (pilot)
Agency: DHS; State, Local, Tribal, Private Sector
Type: Self-Assessment Tool and Training
Tool Assesses: Vulnerability

Through Operation Archangel, a pilot program and partnership between the DHS and the Los Angeles Police Department, assessors in the local police department and the National Guard are trained to conduct vulnerability assessments of critical State and local infrastructure to populate the ACAMS database. This pilot supports local and rural communities in identifying critical assets, assessing vulnerabilities, and developing preparedness programs at the local level. The focus is on collecting and communicating the necessary information required by an incident commander both pre-incident, in terms of protection plans and operational guides, and post-incident, as information required for effective response, mitigation, and recovery. Once these sites are assessed, the data can be supplied through ACAMS, providing improved domain awareness through an information portal. The ACAMS pilot is a secure online database that allows for storing, organizing, and using critical asset assessment information, and deploying that information to first-responders to improve preventive, security, and response activities.

Cross-Border Pipeline Infrastructure Vulnerability Assessments

Tool: Pipeline Assessment Tool
Agency: DOE; TSA
Type: Government Site Assessment
Tool Assesses: Vulnerability

The DOT and TSA are working with the DHS and DOE to gain domain awareness of the Nation's pipeline infrastructure system, identify vulnerabilities in U.S. and cross-border pipeline infrastructure, and review pipeline industry security plans and programs. TSA's Pipeline Security Division, along with pipeline security agencies from Canada, is participating in conferences and pipeline facility visits to assess the assets, threats, and vulnerabilities of the trans-border pipeline systems. TSA is the lead agency working with the DHS Office of Intelligence and Analysis (I&A) and the DOE Office of Energy Assurance (OEA), through the Smart Border Declaration's Energy Sector Working Group to deter terrorists from attacking the trans-border energy infrastructure through heightened domain awareness and improved security posture along national borders. Additionally, TSA coordinates tri-national pipeline vulnerability assessment visits with DOE/OEA, DHS/I&A, and Canadian and Mexican government agencies to evaluate cross-border pipeline operators' security plans and emergency response readiness.

Facility Security Management Program (FSMP)

Tool: Aviation Risk Assessment
Agency: DHS; FAA; DOT
Type: Government-Assisted Assessment Tool
Tool Assesses: Risk

Facilities are prioritized based on the impact that damage, loss of a facility, or disruption of the operation would have on air traffic. Included in the prioritization is how readily the asset or the function it performs can be replaced. The assessment of the facility's criticality (or priority) and other risk factors are then translated into facility security levels that drive the minimum required security measures for that facility. To determine the risk level of a particular facility, a systematic assessment of the threat and vulnerability is conducted. This evaluation includes a valid intelligence assessment of the general terrorist threat and an evaluation of any specific terrorist threat information available. Additionally, criminal threat evaluation is conducted by researching verified reportable incidents and criminal statistical data.

The overall results of the analysis are formulated into a risk rating for each facility. This risk rating is then used to determine what types of security measures are needed and whether additional security measures are required for a particular facility. A comprehensive program of scheduled and unscheduled on-site facility security assessments and inspections is conducted to ensure that the facility has implemented the required security measures based on its prioritization and threat assessment. If all required security measures have been fully implemented, then the facility is issued accreditation. If all required security measures have not been implemented, then a set of findings are developed and tracked until appropriate resources can be applied to implement the measures. Compliance is continually monitored through a comprehensive program of scheduled and unscheduled facility security assessments and inspections.

Federal Aviation Administration (FAA) Information Systems Security Program (ISSP)

Tool: Aviation Risk Assessment
Agency: DHS; FAA; DOT
Type: Government-Assisted Assessment Tool
Tool Assesses: Risk

The ISSP covers all air traffic control systems, including the operational, mission support, and business/administrative elements. There are six phases to the ISSP, and each phase is applied to implemented systems:

1. **Assessment.** During the assessment phase, information is gathered about a system and a risk assessment is performed. Then, recommendations are developed to mitigate or remediate identified risks.
2. **Security Planning.** During the security planning phase, the system architecture, information sensitivity, and management and operational controls needed to safeguard the system are determined.
3. **Remediation.** During the remediation phase, changes are made to the system based on the risk management/remediation recommendations. The system also undergoes testing to help identify any residual risks that may remain.
4. **Certification.** During the certification phase, the designated approving authority for the system determines whether the residual risks are acceptable and whether the system should be authorized for operational use.
5. **Deployment and Commissioning.** During deployment and commissioning, agreements are reached with other organizations for making specific changes to the system to enable it to connect and interoperate with other air traffic control systems and networks.

10. **Post-Authorization.** The last phase, the post-authorization phase, is to ensure that the system continues to operate as intended and that no new risks have arisen or been introduced.

Federal Highway Administration (FHWA) Bridge and Tunnel First-Responder Workshops

Tool: First-Responder Awareness to Terrorist Threats for Bridges and Tunnels Workshop
Agency: DOT; FHWA
Type: Government Instruction on the Identification of Threats and Vulnerabilities to Bridges and Tunnels and Mitigation Approaches
Tool Assesses: First-Responder Threat Awareness

The ½-day-long workshop is designed to give first-responders, such as law enforcement personnel, inspectors, and other emergency responders, an overall awareness of terrorist threats and structural vulnerabilities. More specifically, they will learn to identify the strengths and weaknesses of bridge and tunnel components, estimate the damage to be expected for terrorist threats, and analyze the risk of each component to a specific threat. Threats covered include the vehicle-borne improvised explosive devices (IEDs), hand-placed IEDs, non-explosive cutting devices, fire, and vehicle impact.

Federal Highway Administration (FHWA) Bridge and Tunnel Vulnerability Workshops

Tool: FHWA Risk Management for Terrorist Threats to Bridges and Tunnels Workshops
Agency: DOT; FHWA
Type: Government Instruction on Assessment Tool Usage
Tool Assesses: Vulnerability and Risk by Design

The Risk Management for Terrorist Threats to Bridges and Tunnels Workshop is 1½ days long and is designed to give engineers and managers the understanding to develop a cost-effective risk management plan for a structure using component-level analysis. More specifically, they will learn to identify strengths and weaknesses of bridge and tunnel components, estimate the damage to be expected for terrorist threats, and analyze the risk of each component with regard to a specific threat. Threats covered include vehicle-borne IEDs, hand-placed IEDs, non-explosive cutting devices, fire, and vehicle impact.

Federal Highway Administration (FHWA) Statewide and Project-Specific Vulnerability Assessments

Tool: Highway, Bridge, and Tunnel Vulnerability Assessments
Agency: DOT; FHWA
Type: Government-Assisted Site Visit Assessment
Tool Assesses: Vulnerability

An FHWA-trained cadre of engineers stands ready to assess bridges and tunnels for vulnerability to terrorist threats. DOT engineers, at the request of State transportation leaders, assess the vulnerabilities of highway assets (signature bridges, tunnels, and key intermodal freight transfer facilities; traffic control systems) and prioritize security needs. This Engineering Assessment Team (EAT) performs assessments, at the request of the owners, for project-level, facility-level, and statewide critical structures. To date, the aim has been to guide the owners and operators to identify vulnerable components and recommend measures to reduce those vulnerabilities. The team also provides technical support to the USCG for its port security assessments.

Freight Analysis Framework (FAF)

Tool: FAF Version 1
Agency: DOT; FHWA
Type: Government-Conducted Analysis Tool
Tool Assesses: Consequence

FAF acts as a surface transportation consequence analysis tool to estimate commodity flows and related transportation activities among State, sub-State regions, and major international gateways on the Nation's transportation infrastructure facilities. FAF

identifies how commodities are moved from origin to destination through the highway network. It can also be used to conduct scenario analysis with regard to disabling any roadway links (highway segment, bridges) and nodes (interchanges and intersections) covered by the FAF highway network. This scenario analysis produces a number of key insights, including identifying critical nodes in the surface transportation arena, possible alternative routes, the number of affected trucks, congestion both upstream and downstream of the affected links/nodes, tonnage and dollar value of the commodities affected, types of commodities being affected, additional travel time, and a new congestion outlook throughout the network. The highway network where these commodities are transported includes all interstate highways and all principal arterials. The network covers more than 450,000 miles of roadway.

The FAF commodity data are measured in terms of annual average daily movement. Any analysis based on such data is an assessment for a typical average day. It takes substantial effort to organize both the network and commodity origin destination data to run an FAF scenario analysis. For a single scenario analysis, it is expected to take a minimum of a full workday. Currently, FHWA is updating the original FAF (FAF1) to provide more accurate and complete pictures of freight movement in the Nation. While FAF2 is under development, FAF1 is still operational.

Hazard Analysis and Critical Control Points (HACCP) Methodology

Tool: HACCP (for freight rail; piloting for long-distance passenger rail)
Agency: TSA
Type: Government-Conducted Analytic Methodology
Tool Assesses: Risk

TSA uses a system-oriented risk HACCP methodology to determine the security risks associated with movement of maritime containers and toxic inhalation hazard (TIH) chemicals by rail. HACCP, and its accompanying metrics, was a collaborative development effort drawing on expertise from the DHS and DOT, with the input of numerous railroad career specialists and subject matter experts with perspectives ranging from railway industry management, security, and regulatory oversight. This methodology provides a process for determining which points in a particular freight rail system are the most critical to protect and offers a general view of security options to control the catastrophic breach of a TIH railcar exposing hazardous cargo to the atmosphere. The analysis focuses on using explosives to cause the TIH breach; however, other means are also assessed. The analysis also captures the potential consequences and plume size of the release. The methodology accounts for physical security measures, the critical node's infrastructure characteristics, impact on rail operations, symbolic importance, proximity to other CI/KR, and other variables. Surface Transportation Security Inspectors are also adapting a version of HACCP that FTA uses for application with long-distance passenger rail, as well as a more involved impact analysis for implementing different types of countermeasures.

Hazardous Materials Transportation Risk Management Self-Evaluation Framework

Tool: Risk Management Self-Evaluation Framework (RMSEF) Security Template
Agency: DOT; Pipeline and Hazardous Materials Safety Administration (PHMSA)
Tool Assesses: Vulnerabilities and Strategies to Mitigate Risks

PHMSA's Hazardous Materials Regulations (HMRs) require shippers and carriers of certain hazardous materials to develop and implement security plans that consider risks related to transportation of hazardous materials in commerce. The security plan must address personnel security, en route security, and unauthorized access. Shippers and carriers subject to the security plan requirement must perform an assessment of the transportation security risk associated with the materials they handle. The RMSEF Security Template provides principles and structure illustrating how a risk management methodology can be used to identify points in the transportation process where security procedures should be enhanced within the context of an overall risk management strategy.

IDEF0

Tool: IDEF0 (Integration Definition for Functional Modeling)
Agency: Department of Commerce, FIPS 183
Type: Self Assessment
Tool Assesses: Organizational Processes and Functions

IDEF0 (Integration Definition Language 0) is based on the Structured Analysis and Design Technique (SADT) and includes both a definition of a graphic modeling language and a description of a comprehensive methodology for developing models for a wide variety of automated and non-automated systems. It is comprehensive and expressive, capable of representing a wide variety of business, manufacturing, and other types of enterprise operations to any level of detail. IDEF0 provides a means for completely and consistently modeling the functions required by a system or subject area and the data and objects that interrelate with those functions.

Joint Vulnerability Analysis (JVA)

Tool: Joint Vulnerability Analysis
Agency: TSA (with FBI assistance as needed)
Type: Government-Conducted Field Assessment
Tool Assesses: Vulnerability

JVA will be applied at all commercial airports, focusing initially on the nationally critical airports. As required by legislation, JVA is applied jointly by TSA Aviation Operations personnel and FBI personnel. JVA uses current, FBI-developed threat information as its starting point and then focuses on defining an airport's security system in detail. Once the airport's security system is defined, JVA examines the security system against a current threat required to complete the given threat. Using a ViSAT-shell for the assessment, once the airport's security system is defined, JVA focuses on examining security system against current threats.

Maritime Security Risk Assessment Model (MSRAM)

Tool: MSRAM
Agency: USCG
Type: Government-Applied Risk Assessment Tool
Tool Assesses: Threat, Vulnerability, Consequence, and Risk

MSRAM is a risk analysis tool used to analyze strategic, operational, and tactical risks within and across U.S. ports that allows risk managers and decisionmakers to understand the geographic density of risk across the Nation's ports, the profile of risk within a port, and asset-specific risk to help identify maritime CI/KR. The tool is designed to allow a port-level user to assess risk based on the threat, vulnerability, and consequence factors associated with a target (asset) in the maritime domain. The assessor uses scenarios, pairing an asset and attack mode in combination. Each scenario is analyzed to determine threat, vulnerability, consequence, area-wide security, and response capabilities.

Threat is computed using data from the USCG Intelligence Coordination Center using terrorist intent and capability. Consequence is computed by analyzing the primary consequence and the secondary economic impact of an attack. In the analysis, the following factors are considered: death and injury, primary economic impact, symbolic effect, national security, environmental impact, response capabilities, recoverability, redundancy, and secondary economic impact. Vulnerability is computed by analyzing the achievability of the attack, system security, and target hardness. Local risk data are collected in such a way that it can be used to inform both local and national risk analysis needs and feed the risk management process within the maritime domain.

Multi-Modal Criticality Tool (MMCT)

Tool: MMCT
Agency: TSA
Type: Government-Conducted Assessment Tool
Tool Assesses: Consequence

TSA's strategic risk assessment approach begins by assessing *consequences* to identify assets that are most important to protect from attack. Starting with the former FBI National Infrastructure Protection Center (NIPC) tool, TSA worked with the DHS/IP to develop MMCT in 2003. MMCT provides an assessment of a target's potential importance and the consequences of a worst case, plausible threat. The rating scheme considers aspects from five categories of consequence (e.g., loss of life, economic impact). Criticality determinations are not solely numbers driven; human experience is taken into consideration using a subject matter expert review panel before headquarters analysts make a final determination. Over the last 2 years, TSA has completed more than 2,500 criticality assessments, including one on the Nation's major commercial airports. Applying MMCT to transportation assets was an integral element in determining the Top 100 list of the Nation's critical transportation infrastructures, an effort completed in full collaboration with DOT, USCG, and USTRANSCOM.

Risk Analysis and Management for Critical Asset Protection (RAMCAP)

Tool: RAMCAP Module for Transportation
Agency: DHS
Type: Government-Facilitated Risk Assessment Tool
Tool Assesses: Vulnerability, Consequence, and Risk; Threat provided by the DHS/HITRAC

The DHS is currently developing RAMCAP, a risk framework that the owners and operators of the Nation's critical infrastructure can use to assess terrorist risk to their own assets and systems. This will allow the DHS to normalize and prioritize assets across all 17 critical infrastructure sectors. This process allows owners and operators—who are most cognizant of asset composition and security—to provide the bulk of the information for consequence and vulnerability, given that the DHS provides any of the attack scenarios. The DHS, in turn, will provide an estimate of threat likelihood, representing the judgment of the intelligence community for relative possibility of various attacks against assets of certain types, which will figure critically in owner/operator and DHS evaluations of risk associated with a particular asset. RAMCAP development currently resides with the American Society of Mechanical Engineers (ASME). The DHS is currently using RAMCAP in the Nuclear Reactors, Materials, and Waste Sector and piloting the tool in the Chemical Sector. To date, no RAMCAP transportation modules have been developed, but their development is being planned.

RAMCAP can be considered an asset-driven approach to evaluating risk, since the intrinsic qualities of an asset, rather than the likelihood of a threat, govern the evaluation. Consequence and vulnerability estimates will remain relatively static; variables relative to threat likelihood can be periodically updated to account for the risk-reduction impact of security measures. RAMCAP results allow the DHS and other Federal agencies to prioritize assets from different sectors based on comparative risk analyses. This will, in turn, allow the DHS and other agencies to implement security measures and employ our Nation's resources in a manner that maximizes the allocation of limited resources for the security of the Nation.

Site Assistance Visits (SAVs)

Tool: SAV
Agency: DHS (RMD)
Type: Government-Conducted Assessment
Tool Assesses: Vulnerability

The SAV is an inside-the-fence vulnerability assessment that addresses both the static and dynamic vulnerabilities of a particular site. The SAV is also designed to facilitate vulnerability identification and mitigation discussions between government and industry in the field. It is a qualitative and easy-to-use process that leverages proven techniques; expert knowledge; facility-specific data; hands-on exercises; and all available information, including previously conducted vulnerability assessments. Fifty-three SAVs have been completed in the sector, including aviation, passenger rail, freight rail, and highway bridges and tunnels.

Transit Risk Assessment Module (TRAM) Tool Kit

Tool: TRAM (MAST for maritime application)
Agency: DHS G&T; State and Local Authorities
Type: Self-Assessment Tool
Tool Assesses: Risk

The DHS developed TRAM (and the Maritime Analysis Support Tool (MAST)) to provide a comparative assessment of risk between critical mass transit assets to assist owners and operators in the challenge of prioritizing scarce resources. The DHS developed the tool kit using a best practices approach of risk assessment methods from throughout the Federal Government. This self-assessment tool provides methods for owner/operators to conduct consequence, threat, vulnerability, response and recovery, and impact assessments. Finally, these results can inform a risk assessment, allowing the assessor to prioritize needs and resources. While the tool measures risk on a relative basis, such as the likelihood of one attack type occurring versus another, this tool does not make direct dollar-to-dollar cost-benefit comparisons.

Transportation Security Administration (TSA) Corporate Security Reviews (CSRs)

Tool: CSR
Agency: TSA
Type: Government-Assisted Self-Assessment Tool
Tool Assesses: Vulnerability, Consequence, and Risk (when Threat is provided by TSA)

The CSR process assists TSA risk assessors in identifying risks, preparing mitigation strategies, and prioritizing security needs. The CSR process is used with the goal of hosting face-to-face meetings with key stakeholders to review their security plans. This process helps TSA and the DHS to better identify the assets at greatest risk across the country and improve their security capabilities. CSR objectives include efforts to validate implementation of corporate security plans, gather data for intra/intermodal trend analysis, identify security gaps and offer mitigation options, and promote domain awareness and outreach to sector stakeholders. TSA's CSR program has reviewed more than 60 percent of State departments of transportation, and has been expanded to pipelines and motor carriers of freight and passengers, including schoolbus operations. CSR visits serve to collect physical and operational preparedness information, critical assets, and key point-of-contact lists; review emergency procedures; conduct domain awareness training; and provide an opportunity to share industry best practices. TSA's program is instructive for all entities engaged in transportation by motor vehicle or those that maintain or operate key physical assets within the highway transportation and pipeline community. The CSR is a voluntary event and is conducted at the invitation of the owner or operator of the physical structure or operating entity. CSR files serve as the only universal baseline security data repository available within the partnership of Federal agencies and they assist in developing security standards and measuring compliance.

Vulnerability Identification Self-Assessment Tool (ViSAT)

Tool: ViSAT
Agency: TSA
Type: Self-Assessment Risk Assessment Tool
Tool Assesses: Vulnerability, Consequence, and Risk (Threat provided by TSA)

ViSAT is a voluntary Web-based, self-assessment tool that guides a user through a series of security-related questions to develop a comprehensive security baseline evaluation of a transportation entity's current level of security. ViSAT focuses on the prevention and mitigation of a base array of threat scenarios developed for various subcategories of transportation modes, known as ViSAT modules.

These owner/operator-conducted self-assessment risk modules enable users to assess their baseline security system's effectiveness in direct response to specific threat scenarios. Users are required to rate their asset in terms of target attractiveness (from a terrorist's perspective) and several consequence categories that broadly describe health and well-being, economic consequence, and the symbolic value of the vessel or facility. The security system's effectiveness is then reassessed based on the asset's baseline security countermeasures for each threat scenario and then rated on the effectiveness of each countermeasure in detecting and preventing the terrorist's actions under heightened threat conditions corresponding to the Homeland Security Advisory System (HSAS).

The assessment is Web-based, allowing for easy uploading of information to TSA for more indepth analysis by TSA personnel, if desired. Once an assessment has been submitted to the DHS and approved, the information from that assessment will be linked to individual assets, and the system will allow the owner/operator to replicate like assets. The DHS has already deployed ViSAT for targeted maritime vessel and facility categories. The DHS intends to develop ViSAT modules for each of the remaining four transportation modes as well: Aviation, Highway, Freight Rail, and Pipeline. The ViSAT modules for mass transit (heavy rail); passenger rail; and highway bridges, operations centers, and rail passenger terminals are currently available.

Countermeasures deployed during a target-specific alert may have a detrimental effect on the asset's operations. The intention of the defined enhanced countermeasure set is to increase security effectiveness compared to the baseline security effectiveness ratings. Additional or enhanced countermeasures can be included in the security plan, along with estimated resource requirements and a timeframe for implementation. All assessments that are submitted will be verified for accuracy and consistency when compared against like assets. This verification process helps ensure that the data captured are accurate, and it assists users in avoiding potential pitfalls in their process.

Appendix 4: Additional Federal Security Partners

- **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 (COCOM). 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 (JFCC-ISR) to create a system-of-systems JIOC enterprise network-enabled by enterprise information technology architecture.
- **Department of Agriculture (USDA).** USDA sets public policy to protect the Nation's food supply, agricultural base, and natural resources. On January 30, 2004, 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 the DHS, USDA, and the Department of Health and Human Services in expanding and conducting vulnerability assessments, mitigation strategies, and response planning. Since there are key interdependencies between the Transportation Systems Sector and the Food and Agriculture Sector and its component agencies (USDA, FDA), future planning efforts must consider integrating security policies and initiatives where appropriate between the two sectors.
- **Department of Commerce (DOC).** DOC's National Institute of Standards and Technology (NIST) is conducting more than 75 projects that support law enforcement, military operations, emergency services, airport and building security, and cyber security. DOC's National Telecommunications and Information Administration (NTIA), through its research and engineering laboratory, is developing better communication systems for first-responders, improving public safety networks, and researching new uses of the Internet for public safety communications.
- **Department of Justice (DOJ).** DOJ investigates and prosecutes criminal offenses and represents the Federal Government in litigation. The major investigative agencies—the FBI, the Drug Enforcement Administration (DEA), and the Bureau of Alcohol, Tobacco, Firearms, and Explosives—prevent and deter crime and apprehend criminal suspects. DOJ will contribute to the Transportation Systems Sector through its law enforcement role. In the national effort to identify, prevent, and prosecute terrorists within the Transportation Systems Sector, TSA will work closely with the FBI, who 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 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 security issues with foreign governments and addressing issues concerning the security of pipelines that cross national boundaries.

- **Federal Law Enforcement Training Center (FLETC).** FLETC provides basic and advanced training for Federal law enforcement agency personnel at the DHS and DOT. FLETC also provides training for State and local law enforcement officers and other security personnel.
- **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 efforts for food/agricultural product transportation. Since there are key interdependencies between the Transportation Systems Sector and the Food and Agriculture Sector and its component agencies (USDA, FDA), future planning efforts must consider integrating security policies and initiatives where appropriate between the two sectors.
- **Homeland Infrastructure Threat and Risk Analysis Center.** HITRAC is the DHS's 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 DHS's largest investigative bureau. ICE includes the investigative and intelligence resources of the former U.S. Customs Service, the former Immigration and Naturalization Service, and the Federal Protective 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.
- **National Counterproliferation Center (NCPC).** NCPC coordinates strategic planning within the intelligence community 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 intelligence community 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 intelligence community to identify long-term proliferation threats and requirements, and to develop strategies to ensure that the intelligence community is positioned to address these threats and issues. NCPC reaches out to elements both inside and outside of the intelligence community, and the government to identify new methods or technologies that can enhance the capabilities of the intelligence community 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.
- **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 warning of maritime threats or attacks against North America.
- **Office of Intelligence and Analysis.** The DHS's Office of Intelligence and Analysis 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.

- **Office of Naval Intelligence (ONI).** ONI supports joint operational commanders with a worldwide organization and an integrated workforce of active duty, reserve, officer and enlisted, and civilian professionals. At the National Maritime Intelligence Center (NMIC), ONI brings military and civilian employees into a single command to provide "one-stop shopping" for national-level maritime intelligence.
- **Science and Technology Directorate (S&T).** S&T is the primary R&D arm of the DHS. It provides Federal, State, and local officials with the technology and capabilities to protect the homeland.
- **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.
- **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 United States, 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.

Appendix 5: National Asset Database Transportation Taxonomy Quick Reference

11. TRANSPORTATION

- 11.1 AVIATION
  - 11.1.1 Aviation Conveyances
  - 11.1.2 Airports
    - 11.1.2.1 Certificated Airports
      - 11.1.2.1.1 Class I Airports
      - 11.1.2.1.2 Class II Airports
      - 11.1.2.1.3 Class III Airports
      - 11.1.2.1.4 Class IV Airports
    - 11.1.2.2 Non-Certificated Airports
      - 11.1.2.2.1 Public Airports
      - 11.1.2.2.2 Private Airports
    - 11.1.2.3 Military Airfields
      - 11.1.2.3.1 Air Force Airfields
      - 11.1.2.3.2 Army Airfields
      - 11.1.2.3.3 Navy Airfields
      - 11.1.2.3.4 Marine Corps Airfields
      - 11.1.2.3.5 Coast Guard Airfields
    - 11.1.2.4 Foreign Airports
  - 11.1.3 Air Traffic Control and Navigation Facilities
    - 11.1.3.1 Air Route Traffic Control Facilities
    - 11.1.3.2 Airport Traffic Control Towers
    - 11.1.3.3 Flight Service Stations
    - 11.1.3.4 Other Air Traffic Control Facilities
  - 11.1.4 Space Transportation Facilities
    - 11.1.4.1 Military Facilities
      - 11.1.4.1.1 Launch Vehicles
    - 11.1.4.2 Commercial Facilities
      - 11.1.4.2.1 Launch Vehicles
  - 11.1.5 Aviation Sector Command Control Communication Coordination Facilities
  - 11.1.6 Other Aviation Facilities
- 11.2 RAILROAD
  - 11.2.1 Railroad Conveyance
    - 11.2.1.1 Freight Conveyance
    - 11.2.1.2 Passenger Conveyance
      - 11.2.1.2.1 Passenger Trains Long Distance/Intercity
      - 11.2.1.2.2 Passenger Trains Commuter
  - 11.2.2 Railroad Rights of Way
    - 11.2.2.1 Railroad Track
      - 11.3.2.2.1 Truck Terminal HAZMAT
      - 11.2.2.1.1 STRACNET Track
      - 11.2.2.1.2 Other Track
    - 11.2.2.2 Railroad Bridges
    - 11.2.2.3 Railroad Tunnels
  - 11.2.3 Railroad Yards
    - 11.2.3.1 Rail Yard – Local
    - 11.2.3.2 Rail Yard – Classification
    - 11.2.3.3 Rail Yard – Intermodal
    - 11.2.3.4 Rail Yard – HAZMAT

11.2.4 Railroad Stations

11.2.4.1 Railroad Passenger Stations

11.2.5 Railroad Operations Centers

11.2.5.1 Railroad Dispatch and Operations Control Centers

11.2.5.2 Railroad Communications Centers

11.2.5.3 Railroad Signaling Facilities and Equipment

11.2.6 Other Railroad Facilities

11.3 ROAD

11.3.1 Roadways and Supporting Facilities

11.3.1.1 Roadways

11.3.1.1.1 Limited Access Highways

11.3.1.1.2 Multi-Lane Non-Limited Access Highways

11.3.1.1.3 Two-Lane Numbered Highways

11.3.1.1.4 Other Roads

11.3.1.2 Road Bridges

11.3.1.3 Road Tunnels

11.3.1.4 Highway Rest and Service Areas

11.3.1.4.1 Highway Rest Stops

11.3.1.4.2 Highway Service Areas

11.3.1.4.3 Vehicle Weigh Stations

11.3.1.5 Road Transportation Support Facilities

11.3.1.5.1 Operations and Traffic Management Centers

11.3.1.5.2 Road International Border Facilities

11.3.1.5.3 Motor Vehicle Fueling Stations

11.3.2 Trucking

11.3.2.1 Truck Conveyance

11.3.2.2 Truck Terminals Facilities

11.3.2.2.2 Truck Terminal Non-HAZMAT Facilities

11.3.2.3 Truck Rental Facilities

11.3.2.4 Truck Dispatch Centers

11.3.2.5 Truck Operations Centers

11.3.3 Over-the-Road Motorcoach System

11.3.3.1 Motorcoach Conveyance

11.3.3.2 Over-the-Road Motorcoach Passenger Terminals

11.3.3.3 Over-the-Road Motorcoach Facilities

11.3.3.3.1 Storage Facilities

11.3.3.3.2 Maintenance Facilities

11.3.3.4 Over-the-Road Motorcoach Operations Centers

11.3.3.5 Over-the-Road Motorcoach Dispatch Centers

11.3.4 School Bus Systems

11.3.4.1 School Bus Conveyance

11.3.4.2 School Bus Routes

11.3.4.3 School Bus Stops

11.3.4.4 School Bus Maintenance Facilities

11.3.4.5 School Bus Dispatch Centers

11.3.4.6 School Bus Communications Centers

11.3.5 Other Road Facilities

11.4 MARITIME

11.4.1 Vessels

11.4.1.1 Shallow Draft Vessels

11.4.1.1.1 Tugs and Towboats

11.4.1.1.2 Small Vehicle/Passenger Ferries

11.4.1.1.3 River Ferries

11.4.1.1.4 Excursion/Tour Boat

11.4.1.1.5 Supply/Work Boat

11.4.1.1.6 Recreational Vessel

11.4.1.1.7 Barge – Tank

11.4.1.1.8 Barge – Hopper

11.4.1.1.9 Barge – Gas

11.4.1.2 Deep Draft Vessels

11.4.1.2.1 General Cargo Ship

11.4.1.2.2 Container Ship

11.4.1.2.3 Dry Bulk Cargo Ship

11.4.1.2.4 Tank Ship

11.4.1.2.5 Gas Carrier Ship

11.4.1.2.6 Roll-On/Roll-Off and Pure Car Carrier

11.4.1.2.7 Cruise Ship

11.4.1.2.8 Large Vehicle/Passenger Ferries

11.4.1.2.9 Medium Vehicle/ Passenger Ferries

11.4.1.2.10 Military Combatant Vessel

11.4.1.2.11 Military Support Vessels

11.4.1.2.12 Other Vessels

11.4.2 Ports

11.4.2.1 Shallow Draft Ports

11.4.2.1.1 Shallow Draft General Cargo Terminal

11.4.2.1.2 Shallow Draft Dry Bulk Cargo Terminal

11.4.2.1.3 Shallow Draft Liquid Bulk Cargo Terminal

11.4.2.1.4 Shallow Draft Barge Fleeting Area

11.4.2.1.5 Shallow Draft Passenger Terminal

11.4.2.2 Deep Draft Ports

11.4.2.2.1 Deep Draft General Cargo Terminal

11.4.2.2.2 Deep Draft Containerized Cargo Terminal

11.4.2.2.3 Deep Draft Dry Bulk Cargo Terminal

11.4.2.2.4 Deep Draft Liquid Bulk Cargo Terminal – Crude/Product

11.4.2.2.5 Deep Draft Liquid Bulk Cargo Terminal – Chemical

11.4.2.2.6 Deep Draft Bulk Gas Cargo Terminal

11.4.2.2.7 Deep Draft Industrial Cargo Terminal

11.4.2.2.8 Off-Shore Terminals or Platforms

11.4.2.2.9 Outer Continental Shelf Crude Oil Platforms

11.4.2.2.10 Outer Continental Shelf Natural Gas Platforms

11.4.2.2.11 Cruise Ship Passenger Terminal

11.4.2.2.12 Ferry Terminals

11.4.2.2.13 Military Cargo Terminal

11.4.2.2.14 Military Combatant Vessel Terminal

11.4.2.3 Port Public Access Areas

11.4.3 Waterways

11.4.3.1 Inland Waterways

11.4.3.2 Intracoastal Waterways

11.4.3.3 Canals

11.4.3.4 Locks

11.4.3.5 Dams

11.4.4 Maritime Supporting Facilities

11.4.4.1 Navigation Facilities

11.4.4.1.1 Lighthouses and Beacons

11.4.4.1.2 Buoys

11.4.4.1.3 Electronic Navigation Facilities

11.4.4.2 Emergency Search and Rescue Facilities

11.4.4.2.1 U.S. Coast Guard Marine Emergency Response Facilities

11.4.4.2.2 State and Local Marine Emergency Response Facilities

11.4.5 Other Maritime Facilities

11.5 MASS TRANSIT

11.5.1 Rail Mass Transit

11.5.1.1 Rail Transit Cars

11.5.1.1.1 Heavy Rail Transit

11.5.1.1.2 Light Rail Transit

11.5.1.1.3 Commuter Rail

11.5.1.1.4 Other Rail Transit

11.5.1.2 Rail Transit Passenger Stations

11.5.1.3 Rail Transit Rights of Way

11.5.1.3.1 Rail Transit Track

11.5.1.3.2 Rail Transit Bridges

11.5.1.3.3 Rail Transit Tunnels

11.5.1.4 Rail Transit Yards

11.5.1.5 Rail Transit Dispatch and Operations Control Centers

11.5.1.6 Rail Transit Communications Centers

11.5.1.7 Rail Transit Signaling Facilities and Equipment

11.5.2 Bus Mass Transit

11.5.2.1 Transit Bus Vehicles

11.5.2.2 Transit Bus Routes

11.5.2.3 Transit Bus Terminals

11.5.2.4 Transit Bus Stops

11.5.2.5 Transit Bus Garages

11.5.2.6 Transit Bus Dispatch and Operations Control Centers

11.5.2.7 Transit Bus Communications Centers

11.5.3 Other Mass Transit Systems

11.6 PIPELINES

11.6.1 Crude Oil Pipelines

11.6.1.1 Crude Oil Pipeline Components

11.6.1.2 Crude Oil Pipeline Pumping Stations

11.6.1.3 Crude Oil Pipeline Control Centers

11.6.1.4 Crude Oil Storage

11.6.1.5 Crude Oil Pipeline Hub

11.6.2 Petroleum Product Pipelines

11.6.2.1 Petroleum Product Pipeline Components and Interconnects

11.6.2.2 Petroleum Product Pipeline Pumping Stations

11.6.2.3 Petroleum Product Pipeline Control Centers

11.6.2.4 Petroleum Product Storage

11.6.3 Natural Gas Transmission Pipelines

11.6.3.1 Natural Gas Transmission Pipeline Components and Interconnects

11.6.3.2 Natural Gas Transmission Pipeline Compressor Stations

11.6.3.3 Natural Gas Transmission Pipeline Control Centers

11.6.3.4 Natural Gas Transmission Storage

11.6.3.5 Natural Gas Pipeline Hub

11.6.3.6 Natural Gas Receipt/Delivery Metering Stations

11.6.3.7 Liquefied Natural Gas Storage (Terminal)

11.6.4 Natural Gas Distribution

11.6.4.1 City Gate Stations

11.6.4.2 Natural Gas Distribution Pipeline Networks

11.6.4.3 atural Gas Distribution Control and Dispatch Centers

11.6.4.4 Natural Gas Distribution Storage

11.6.5 Liquid Natural Gas (LNG) Facility

11.6.5.1 LNG Facility – Terminal (Marine)

11.6.5.2 LNG Facility – Liquefaction + Vaporization

11.6.5.3 LNG Facility – Vaporization

11.6.6 Other Pipelines

11.6.6.1 Other Pipeline Components

11.6.6.2 Other Pipeline Pumping Stations

11.6.6.3 Other Pipeline Control Centers

11.6.6.4 Other Pipeline Terminals

11.6.7 Other Pipeline Facilities

11.7 REGULATORY, OVERSIGHT, AND INDUSTRY ORGANIZATIONS

11.7.1 Federal Transportation Agencies

11.7.2 State and Local Transportation Agencies

11.7.3 Transportation Industry Organization

Appendix 6: Protocols and Processes for Assessing Effectiveness and Compliance

This appendix addresses specific requirements of Executive Order 13416, Strengthening Surface Transportation Security. The protocols and processes contained herein describe the Transportation Systems Sector's approach to the assessments required in paragraph 3 of the order. These processes will be refined as the measurement procedures associated with the NIPP and the Transportation Systems SSP are defined.

Protocol for Determining the Effectiveness of Information-Sharing Mechanisms

The information-sharing process is designed to communicate both actionable information on threats and incidents, and information pertaining to overall Transportation Systems Sector status (e.g., plausible threats, vulnerabilities, potential consequences, incident situation, and recovery progress). This is accomplished through the collection, production, and sharing of information that enables timely and effective decisionmaking so that owners and operators, States, localities, tribal governments, and other security partners can assess risks, make appropriate security investments, and take effective and efficient protective actions.

The effective implementation of the NIPP and the Transportation Systems SSP is predicated on active participation by government and private sector security partners in robust multi-directional information sharing. When the Nation's surface transportation owners and operators have a comprehensive picture of threats to the transportation system and its CI/KR and participate in the multi-directional information flow, their ability to assess risks, make prudent security investments, and take protective actions is substantially enhanced. Similarly, when the government is equipped with an understanding of private sector information needs, it can adjust its information collection, analysis, synthesis, and dissemination activities accordingly.

The NIPP and Transportation Systems SSP information-sharing approach constitutes a shift from a strictly hierarchical to a networked model, allowing distribution and access to information both vertically and horizontally, as well as the ability to enable decentralized decisionmaking and actions. The objectives of the networked approach are to:

- Enable secure multi-directional information sharing between and across government and industry that focuses, streamlines, and reduces redundant reporting to the greatest extent possible;
- Implement a common set of communications, coordination, and information-sharing capabilities for all security partners;
- Provide security partners with a robust communications framework tailored to their specific information-sharing requirements, risk landscape, and protective architecture;
- Provide security partners with a comprehensive common operating picture that includes, but is not limited to, timely and accurate information about natural hazards, general and specific terrorist threats, incidents and events, impact assessments, recommended security guidelines, lessons learned, and best practices;

- Provide security partners with timely incident reporting and verification of related facts that the Transportation Systems Sector and other CI/KR owners and operators can use with confidence when considering how evolving incidents might affect their security posture;
- Provide a means for State, local, tribal, and private sector security partners to be integrated, as appropriate, into the intelligence cycle, to include providing inputs to the intelligence requirements development process;
- Enable the flow of information required for security partners to assess risks, conduct risk management activities, invest in security measures, and allocate resources; and
- Protect the integrity and confidentiality of sensitive information.

Figure A7-1: NIPP Information-Sharing Framework

Protocol for Measuring the Effectiveness of Security Information Sharing

Measuring the effectiveness of information sharing requires a multi-dimensional assessment approach that can be implemented by actively engaging the Transportation Systems Sector's security partners. Effective information sharing is an outcome of a number of interrelated, complementary, and dynamic capabilities within the sector that can be best assessed and evaluated by developing metrics against each of the information-sharing dimensions. A sample of some of these dimensions includes the following:

- **Stakeholders:** The interactions of participants involved in an information-sharing initiative;
- **Data/Information:** The quality and pertinence of the information provided to the stakeholders;
- **Business Processes:** The timeliness and execution of the information-sharing initiative; and
- **Technology:** The technological capabilities and appropriate use of tools and mechanisms to implement the information-sharing initiative.

Sector security partners working through the GCCs and SCCs will identify and define the key information-sharing dimensions that will then be used to frame the assessment approach. The timeliness of information exchange through the most critical information-sharing mechanisms will be assessed on an annual basis.

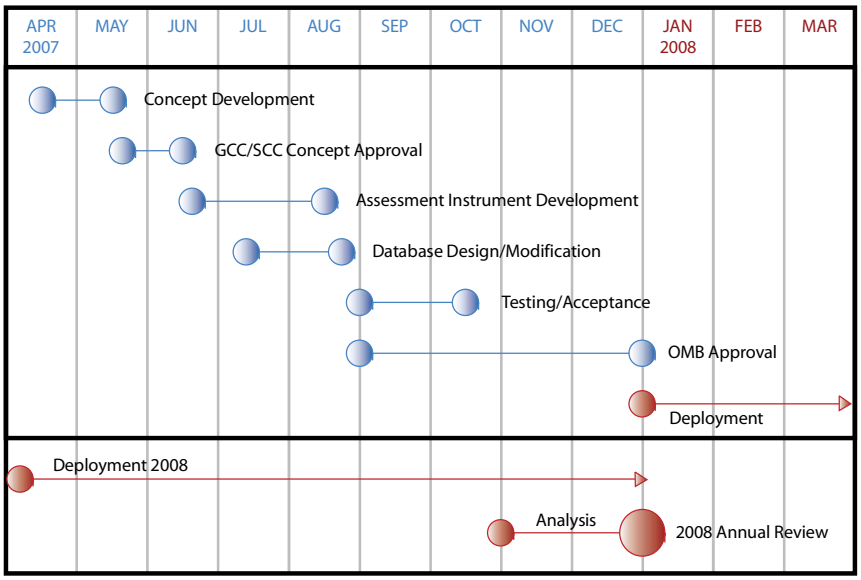
The protocol for measuring effectiveness will align with the Information Sharing Environment Implementation Plan developed under the requirements of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), and with the NIPP and the Transportation Systems SSP measurement requirements. Process measurement data will also be used where the sector has access to such information.

Consistent with Executive Order 13416, Strengthening Surface Transportation Security, this protocol will initially focus on timeliness since the determination of future effectiveness measures will be determined and developed at the user's level (GCCs/SCCs) to incorporate metrics and other evaluation procedures to measure progress and assess the effectiveness of information shared.

Schedule for Annual Information-Sharing Mechanism Effectiveness Assessment

The schedule proposed in the table below will be adjusted, as necessary, at the discretion of the sector's security partners through the GCC and SCC venues to conform to the information process metrics and timelines of the NIPP and Transportation Systems SSP implementation initiatives and the requirements of the information-sharing environment.

Figure A7-2: Annual Schedule for Developing and Reviewing Information-Sharing Effectiveness Measures



Process for Evaluating Compliance With and the Need for Revisions of Security Guidelines and Requirements

The security of the Nation's surface transportation is vital and both the public and private sectors share responsibility for its security. More than 85 percent of the Nation's surface transportation assets lie in private hands and there can be no real security for the Nation without highly effective public/private cooperation.

The Federal Government in partnership with the owners of transportation systems and acting through TSA will continue to seek the development of cooperative security measures for the Nation. These partnerships have and will continue to develop voluntary security guidelines. The current set of security guidelines is identified in the modal annexes of the Transportation Systems SSP. In the future, further voluntary guidelines may be developed by TSA in cooperation with industry, its leadership, its communities of interest, modal GCCs, SCCs, the public, and others.

Guidelines may form the basis for rulemaking should rulemaking be seen as necessary. In the way ahead, adherence to cooperatively developed guidelines will be provided by owner certification. To ensure adherence, TSA will review owner-provided certifications and provide random field audits of a statistically significant portion of those certifications by TSA inspectors or their agents.

When the needs of the Nation demand mandatory security requirements because of acts of terrorism, failure to meet voluntary guidelines, threat information, congressional mandates, court decisions, Executive Orders, petitions for rulemaking, or the like, TSA will act according to its responsibility granted under Public Law 107-71 and seek remedy under its rulemaking authority.

The continuing effectiveness of measures taken to ensure security within the Nation's transportation system requires review as the threats and measures of terrorism continually evolve. Under the guidelines of the Transportation Systems SSP, using NIPP metrics to compare performance to goals, security partners will adjust and adapt the Nation's CI/KR approach to account for progress achieved, as well as for changes in the threat environment. Among actions to ensure the continuing effectiveness of security measures, TSA and the Transportation Systems Sector communities of interest, as outlined in their Transportation Systems SSP modal plans, provide a schedule to meet regularly as GCCs and SCCs to review all security measures in place.

Modal Annexes

Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan

May 2007

Homeland Security

Annex A. Aviation

1 Executive Summary

The comprehensive increase in measures to enhance aviation security following September 11, 2001, led to significant improvements in existing security processes, operations, and technologies in each area of the aviation transportation system. These efforts led to the current security posture of a multilayered, scalable, and flexible aviation security system that is responsive to varying threat levels, as well as to the entire range of identified threats. This has effectively reduced vulnerabilities within the aviation transportation system. However, the ever-changing aviation threat environment continues to challenge the Federal Government and private industry to implement additional effective and efficient security measures.

As directed by the National Infrastructure Protection Plan (NIPP), the Transportation Systems Sector-Specific Plan (SSP) represents the combined planning contributions of the sector's security partners to develop a system-wide approach to reducing the security risks within and across the transportation modes. The aviation mode's security partners include the Department of Homeland Security's (DHS's) Transportation Security Administration (TSA), the Department of Transportation's (DOT's) Federal Aviation Administration (FAA), the Department of Defense (DoD), the Department of Justice (DOJ), airlines, airports, flight crews, air cargo industry members, State and local law enforcement, and passengers.

This Aviation Implementation Plan has been developed in concert with the emerging National Strategy for Aviation Security (NSAS) and its supporting implementation plans. The NSAS provides an overarching national strategy necessary to optimize the coordination and integration of government-wide aviation security efforts. This Transportation Systems SSP Aviation Implementation Plan shares several common goals with the NSAS that purposely help to define an overarching framework for achieving the objectives of the NIPP. These common goals include calling on the Nation to use the full range of its assets and capabilities to prevent the air domain from being exploited by terrorist groups, hostile nation-states, and criminals to commit acts against the United States, its people, infrastructure, and other interests; ensuring the safe and efficient use of the air domain; and calling on the Nation to continue using the air domain for air travel and commerce.

The Transportation Systems SSP aviation modal vision is to achieve a secure, resilient, and efficient network of airlines; other aviation operators; airports; personnel; and infrastructure to ensure the safe and efficient movement of people and cargo and to prevent exploitation of the aviation transportation system to carry out attacks. Supporting this vision are partnerships between government and private sector entities, and a threat-based, risk-managed approach to enhance security measures that recognize the mode's diversity.

This Aviation Implementation Plan associates current programs within the aviation community with the Transportation Systems Sector security goals and key objectives. The plan also identifies approaches for determining the way forward in aviation system security. The NIPP risk management framework, outlined in the Transportation Systems SSP Base Plan, is used to facilitate identification and prioritization of critical systems and assets, which informs and assists program development. Risk

mitigation options, including physical, process, and institutional changes, will be considered for these systems and assets, and prioritized based on their alignment with Transportation Systems Sector security goals, research and development (R&D) strategic goals, and other guidance from sector stakeholders.

The comprehensive implementation of a risk management methodology for the aviation transportation system will result in a prioritized portfolio of risk mitigation activities that will be informed and updated based on relevant risks to the mode. Through the partnership already established between government and industry, enhancements to the aviation security posture will be effected in consultation with all aviation security partners. Security shortfalls and subsequent funding deficiencies will be identified through this process. In addition, government aviation security resources will be leveraged in conjunction with those of industry to minimize cost and coordinate modal security enhancements.

With a view toward this end-state, the Transportation Systems SSP Base Plan and this Aviation Implementation Plan specifically focus on how the Transportation Systems Sector will continue to enhance the security of its critical infrastructure and key resources (CI/KR). Programs to protect the aviation system are key to making the Nation safer, more secure, and more resilient in the face of terrorist attacks and other hazards.

It is with these goals and objectives in mind that the following plan is respectfully presented.

2 Overview of Mode

For aviation transportation system security purposes, the aviation mode comprises a broad spectrum of public and private sector elements. The mode's diversity and complexity require an integrated and flexible approach to security. The mode's core components are the National Airspace System (NAS), commercial airlines, charter operators, airports, general aviation, and air cargo.

Federal departments and agencies are responsible for establishing and enforcing regulations, policies, and procedures; providing criminal law enforcement; identifying potential threats and appropriate risk-managed countermeasures; defining and mitigating risks and vulnerabilities on the ground and in the air; providing overall guidance; and applying security measures to passengers, their carry-on items, flight crew, baggage, and cargo. Airlines, airports, flight crews, air cargo industry members, State and local law enforcement, and passengers also play key roles in the multi-layered protective posture that has taken aviation security beyond where it stood on September 11, 2001.

The Department of Homeland Security's (DHS's) Transportation Security Administration (TSA) oversees aircraft operators, foreign air carriers, and airport security; provides criminal law enforcement; and cooperates with State and local governments, local airport authorities, and law enforcement agencies to ensure the security of aviation operations and facilities. The Department of Transportation (DOT), through the Federal Aviation Administration (FAA), provides regulatory oversight for and operates the NAS as the country's civil aviation authority and air navigation services provider. The FAA, in cooperation with the DHS and other security partners, plans and implements diverse air traffic and airspace management-related measures to support national defense, homeland security, law enforcement, and national response efforts. In addition, FAA is responsible for securing manned and unmanned NAS facilities and systems. These entities, along with other government agencies and the private sector, have collaborated in preparing this Aviation Implementation Plan (see section 2.3).

2.1 Vision of Mode

The aviation modal vision is to achieve a secure, resilient, and efficient network of airlines; other aviation operators; airports; personnel; and infrastructure to ensure the safe and efficient movement of people and cargo and to prevent exploitation of the aviation transportation system to carry out attacks, while protecting the civil liberties of all individuals. This vision will be supported by partnerships between government and private sector entities and by a threat-based, risk-managed approach to risk mitigation that recognizes the mode's diversity.

2.2 Description of Mode

The aviation mode is vitally important to U.S. prosperity and freedom. Each day, commercial aviation moves millions of passengers and their bags through U.S. airports. In 2005, with regard to air cargo, U.S. air carriers flew 39.2 billion revenue ton-miles—16.1 billion domestic and 23.1 billion internationally.[158] Historically, general aviation has accounted for more than 77 percent of all flights in the United States, carrying more than 105 million passengers each year.[159] The various sectors of U.S. aviation provide for transporting passengers and goods vital to the continued health of the national economy.

The components of the aviation mode—NAS, commercial airlines, commercial airports, general aviation, air cargo, and international programs—are discussed in more detail below.

National Airspace System (NAS). NAS is the dynamic network of facilities, systems, regulatory oversight, services, airspace, and routes that supports flights within U.S. airspace, including the international airspace delegated to the United States for air navigation services. FAA regulates and operates this service.

Commercial Airlines. Commercial airlines are regularly scheduled or public charter operations that are regulated under Title 49 of the Code of Federal Regulations (CFR). The regulations apply to both domestic and international operations flying within, from, to, or over the United States. Although commercial operations typically use large transport category aircraft, any type of aircraft—from a piston single-engine aircraft to an intercontinental jet—may be used.

Commercial airports. Commercial airports are defined as airports with regularly scheduled commercial passenger service. Currently, there are approximately 450 commercial airports in the United States that utilize TSA screening resources. The network of civilian and civilian/military joint-use airports is clearly perceived to be an essential resource for the Nation's economic and psychological well-being. Airports are also symbolic of U.S. citizens' expectations of freedom of travel, and are increasingly becoming nodes at which many or all modes of transportation interface.

General Aviation (GA). GA is defined as all segments of the aviation industry other than regularly scheduled commercial air carriers and military aviation. GA's 200,000 aircraft and 630,000 certificated pilots transport 145 million passengers each year and use some 19,000 landing facilities. The GA industry encompasses a wide range of activities, from pilot training to flying for business and personal reasons, charter operations, delivering emergency medical services, firefighting, law enforcement, and sightseeing. Operations range from short-distance flights in single-engine light aircraft to long-distance international flights in corporate or privately owned "wide-bodies" and from emergency aero-medical helicopter operations (i.e., MEDEVAC) to airships hovering over open-air sporting events.

Air Cargo. Air cargo is defined as 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. U.S. mail is not considered cargo and is covered under a separate security program.

International Programs. The TSA International Programs Office is an integral, but unique part of the intricate web protecting the U.S. civil aviation system. The International Programs Office protects international civil aviation at the point of origin en route to the United States or in select upstream locations, with the goal of ensuring freedom of civil aviation operations for people and commerce. The International Programs Office also provides global quality control for civil aviation security and assists in improving the international level of security through maintaining effective business processes for assessments, surveys, air carrier inspections, crisis response, and management, combined with dynamic strategic, tactical, and operational planning.

[158] FAA Aerospace Forecast, Fiscal Years 2006-2017
[159] Aircraft Owners and Pilots Association Data, www.aopa.org/special/newsroom/stats/activity.html.

2.3 Government Coordinating Council/Sector Coordinating Council Structure and Process

In late 2005, the Secretary of Homeland Security exercised his authority under Section 871 of the Homeland Security Act to create a committee, not subject to the Federal Advisory Committee Act (FACA), to facilitate public-private consultation on matters of critical infrastructure protection. Under this umbrella authority, which the DHS Office of Infrastructure Protection exercises, several committees have been formed to focus on protecting critical infrastructure in the Transportation Systems Sector of the national economy. These include a Transportation Systems Sector Government Coordinating Council (GCC) (composed of agencies on all levels of government); a Transportation Systems Sector Coordinating Council (SCC) (composed of representatives of the owners and operators of critical transportation infrastructure); and the Critical Infrastructure Protection Advisory Council (CIPAC), a forum in which the Transportation Systems Sector GCC and the Transportation Systems SCC consult with one another. The Aviation GCC and the Aviation SCC have formed a Joint Aviation Plan Working Group under the auspices of CIPAC. CIPAC acts as a partnership model for the Transportation Systems Sector. CIPAC is responsible for facilitating and coordinating planning; implementing security programs; providing operational activities related to critical infrastructure protection security measures, including incident response, recovery, and reconstitution from events both manmade and naturally occurring; and sharing information about threats, vulnerabilities, protective measures, best practices, and lessons learned.

The membership of the Aviation SCC includes representatives of owners and operators of critical aviation infrastructure. The Aviation SCC acts to establish and implement the public-private partnership envisioned by the National Infrastructure Protection Plan (NIPP). In this effort, the Aviation SCC facilitates outreach and coordination among its stakeholders to coordinate the development of the Nation's aviation security plans with the Aviation GCC. Industry members of the Aviation SCC include organizations such as the Air Transport Association, the Aircraft Owners and Pilots Association, the Boeing Company, the Cargo Airline Association, and the National Air Transportation Association.

Like the Aviation SCC, the Aviation GCC fosters communication across government, as well as between government and private industry, in support of the Nation's homeland security mission. The permanent membership of the Aviation GCC is comprised of senior executives or their designees from TSA, FAA, the DHS Office of Infrastructure Protection, the Federal Bureau of Investigation (FBI), the Department of Defense (DoD), and the National Association of State Airline Officials (designated State government official).

3 Implementation Plan

The three Transportation Systems Sector security goals and supporting objectives described in the Transportation Systems SSP Base Plan apply broadly to the aviation mode. Risk-managed decisionmaking is applied within the aviation mode to determine the actions (programs and processes) necessary to achieve the goals. Achieving these goals relies heavily on a continued partnership between government and industry, with a clear focus on implementing cost-effective, mitigating security measures that are both flexible and unpredictable.

3.1 Goals, Objectives, and Programs/Processes

The Transportation Systems Sector-Specific Plan (SSP) process for identifying sector security goals reflects the collaborative approach of the entire SSP development process, as directed by Homeland Security Presidential Directive 7 (HSPD-7). The Transportation Systems Sector security goals presented in the Base Plan represent the consensus of the sector's security partners. To achieve long-term success in securing the aviation transportation system, the Transportation Systems Sector security goals will need to be seamlessly integrated into a risk-managed decisionmaking framework. In the subsequent paragraphs, the Aviation Implementation Plan associates the Transportation Systems Sector security goals and key objectives with specific programs within the aviation community. A number of regulatory, screening, law enforcement, military, and intelligence activities and programs are in place within the aviation community to attain these objectives. Appendix 1 to this plan lists the aviation programs and the Transportation Systems Sector security goals that they support.

3.1.1 Goal 1: Prevent and Deter Acts of Terrorism Using or Against the Transportation System

The objectives supporting goal 1 are:

- Implement flexible, layered, and unpredictable security programs using risk management principles;
- Increase the vigilance of travelers and transportation workers; and
- Enhance information and intelligence sharing among Transportation Systems Sector security partners.

As evidenced by the August 2006 plot against U.S.-bound flights from the United Kingdom, the large and dynamic aviation transportation system remains an attractive target for terrorists. Many security measures have been implemented or improved since the 9/11 terrorist attacks, and the Federal Government, in cooperation with its stakeholders, continues to work within the changing threat environment to identify and mitigate potential threats and risks to the aviation transportation system. Protecting critical infrastructure is a national and homeland security concern that continues to receive a high degree of attention.

Because of these conditions and based on the Presidential and congressional direction of the Aviation and Transportation Security Act (ATSA), TSA deploys approximately 40,000 highly trained Transportation Security Officers (TSOs), who work at more than 700 security checkpoints and nearly 7,000 baggage screening areas each day in the United States. To ensure effective and efficient operations at airports, the TSO workforce must be well-trained and alert to the latest threats. TSOs follow established screening procedures for processing passengers and carry-on items through passenger screening checkpoints and for processing checked baggage through baggage screening checkpoints.

TSA, in cooperation with FAA, DoD, the Department of Justice (DOJ), and other key stakeholders, continues to strengthen aviation security to protect the United States from threats involving the aviation domain as outlined in the following paragraphs, using the sector goal objectives as a framework.

Objective 1: Implement flexible, layered, and unpredictable security programs using risk management principles.

To adapt to the ever-changing threat environment, a variety of steps may be taken to deal with recognized and unidentified risks. Aviation risks are generally based on two types of threats: the aircraft as a target for attack (e.g., hijacking, stand-off weapons, on-board improvised explosive devices) and the aircraft as a weapon (e.g., as seen on 9/11, or as a delivery vehicle for a weapon of mass destruction (WMD)).

Transportation Systems Sector Systems-Based Risk Management (SBRM) methodology: Using risk management principles, a number of flexible, layered, and unpredictable security programs have been implemented in the aviation domain. The aviation modal risk management approach incorporates the Transportation Systems Sector SBRM methodology. TSA's risk management program will account for both systems-based and asset-based risks. The program will define the mode's risk profile; develop the standards and criteria for a common, relevant operational picture to aid stakeholders to make effective decisions; and generate a portfolio of alternative management strategies that leaders can use to build action and investment agendas that improve the overall risk profile of the mode.

The following are examples of programs that meet objective 1:

- **Federal Air Marshals**. TSA deploys Federal Air Marshals on board U.S. air carriers, both internationally and domestically. With nearly 30,000 U.S. commercial flights each day, TSA employs a risk-based approach in selecting the flights for coverage. This risk-based approach assesses risk as a function of consequence, vulnerability, and threat/intelligence. The Federal Air Marshal Service (FAMS) Mission Operations Center, collocated with the Transportation Security Operations Center (TSOC), provides incident coordination and law enforcement support to FAMS on a 24 hours per day, 7 days per week (24/7) basis. Federal Air Marshals are also assigned to all 56 FBI Field Office Joint Terrorism Task Forces (JTTFs) and the National JTTF, where they are assigned cases based on relevance to the aviation/transportation domain. FAMS coordinates foreign air marshal missions arriving in the United States, facilitates the logistics of these missions, conducts regular liaison with foreign air marshal programs, and conducts train-the-trainer programs for international air marshals.

- **Facility Security Management Program**. By protecting the facilities that constitute the systems that, in turn, provide air traffic services, FAA ensures the operational availability of the NAS. FAA's Facility Security Management Program is a robust program for categorizing and assessing facilities and implementing protective measures. FAA security specialists assigned across the country conduct assessments and inspections at FAA facilities to determine compliance with facility security, communications security and classified information, public laws, national directives, and DOT policies that influence FAA security practices. This creates a security environment within FAA that reduces the risks posed by espionage, sabotage, theft, vandalism, terrorism, and other criminal acts.
- **Hazardous Materials Regulations (HMRs)**. Within the aviation mode, FAA is also responsible for investigating and enforcing HMRs issued by the DOT Pipeline and Hazardous Materials Safety Administration. Most hazardous materials (HAZMAT) transported by air are in small non-bulk packages and are not subject to the HMR security plan requirements, which apply to persons accepting or offering bulk quantities (placarded amounts) of HAZMAT. Air carriers subject to TSA security program requirements are authorized to comply with any air-mode HAZMAT security plan requirements by following their TSA-approved security program. Separately, however, all persons involved in HAZMAT commerce must receive security awareness training in accordance with the HMR.
- **Airport Liaison Agent (ALA) Program**. The FBI, through its ALA program, has FBI Special Agents assigned to each TSA-regulated airport. FBI ALAs support and enhance efforts to prevent, disrupt, and defeat terrorism and criminal operations directed toward civil aviation. Additionally, the ALAs provide counterterrorism preparedness, leadership, and assistance to Federal, State, local, and tribal agencies responsible for civil aviation security.
- **Commercial Airlines**. Commercial airlines must comply with Federal security regulations. The regulatory scheme can facilitate constructive government and industry communication when developing means and mitigation tactics for securing the aviation system. All domestic scheduled commercial airlines are required to follow a standard security program under 49 CFR 1544, depending on the type of operation. These programs are regularly amended to account for the changing threat environment, new technologies and practices, and measures no longer practical.
- **Air Cargo**. The complexity of the air cargo environment necessitates a deliberative risk analysis and consideration of available resources among a wide array of options. The rapid transport of goods by air to destinations throughout the Nation and the world is an essential service. Security measures that are integrated into air cargo operations can help minimize unnecessary delays. TSA seeks to strengthen shipper and supply chain security for vetting sources and integrity in transit; use advanced information technology (IT) to identify elevated-risk cargo through prescreening; identify, develop, and deploy technology and procedures for performing targeted cargo inspections; and inspect 100 percent of targeted cargo.

  TSA's air cargo security final rule codified security upgrades introduced since 9/11, and requires additional security measures throughout the air cargo supply chain. The application of identification and access control requirements in all-cargo aircraft operations areas, screening of persons transported and service personnel who board all-cargo aircraft, and new standard security programs for operators of large all-cargo aircraft are required. TSA issued complete revisions of all aircraft operator and indirect air carrier (IAC) security programs, including comparable requirements for screening cargo and access controls to facilitate transfer of cargo without compromising security standards.

  A number of key initiatives are underway to achieve these goals, including developing the **Freight Assessment System (FAS)**. FAS will screen all air cargo to identify elevated-risk shipments for aircraft operator inspection prior to flight. Data on shippers, agents, IACs, air carriers, consignees, contents of the shipment, and threat information will be incorporated into the risk assessment at a transactional level for domestic and international shipments. TSA is also developing and implementing enhancements to the **Indirect Air Carrier Management System** to process the approval of new and renewal applications for IAC security programs and automate background checks of IAC officials and persons with unescorted access to cargo, as required by the new final rule.

- **General Aviation (GA)**. Because of the size and diversity of the GA industry, TSA uses a threat-based, risk management and consequence analysis approach to security. This means that the agency will analyze credible threat intelligence information to determine and prioritize the risks, threats, and vulnerabilities that exist. Based on this approach, TSA has developed a layered security arrangement, which integrates the capabilities of TSA and the stakeholder community to increase security using diverse and complementary measures rather than relying on a single-point solution, creating programs and policies that are reasonable, feasible, and effective for industry, while maintaining an appropriate level of security. To complement the threat-based, risk management, and consequence analysis approach, TSA has established strong lines of communication and working partnerships with industry stakeholders to support, promote, implement, and develop security programs and policies.

  While the majority of GA is unregulated for security purposes, TSA does regulate certain segments of the industry. Operators of large aircraft (greater than 12,500 pounds maximum takeoff weight) used in charter or all-cargo operations are mandated to comply with the security requirements set forth in one of the TSA-approved standard security programs. Additionally, TSA regulates certain flight activities in the National Capital Region (NCR), such as the **Maryland Three Rule (MD-3)**, which focuses on three small Maryland airports in the Flight Restricted Zone, and the **Restoration of General Aviation at Ronald Reagan Washington National Airport (GA@DCA)**.

  In accordance with TSA Security Directives (SDs), international and domestic commercial aircrews who fly into, out of, and over the United States are required to submit those crews in a Master Crew List (MCL), and in Flight Crew Manifests (FCMs) for each applicable flight for vetting by TSA against terrorism-related watch lists. This function is accomplished through TSA's Office of Transportation Threat Assessment and Credentialing (TTAC).

- **Assistant Federal Security Directors for Law Enforcement (AFSD-LE)**. TSA law enforcement personnel includes AFSD-LE. The consolidated law enforcement presence provides prevention, protection, and response capabilities for TSA in the transportation domain. AFSD-LE's primary duties are to establish and maintain liaison with Federal, State, and local law enforcement authorities, and coordinate their activities within the transportation domain.

- **Visible Intermodal Protection and Response (VIPR) Teams**. Deploying TSA VIPR teams introduces an element of unpredictability to disrupt potential criminal or terrorist planning activities. These mobile teams, consisting of law and civil enforcement personnel, operate in aviation and other transportation systems to detect, deter, and defeat possible terrorist activity. TSA VIPR team deployments are designed to quickly and effectively raise the level of security in any mode of transportation anywhere in the country. The teams work with local security and law enforcement officials to supplement existing security resources and provide deterrent presence and detection capabilities.

- **TSA National Explosives Detection Canine Team Program**. This program prepares and deploys hundreds of dogs to serve with State, regional, and local airport law enforcement authorities. These mobile teams can quickly locate and identify dangerous materials that may present a threat to transportation systems and can be used in all areas of the airport environment. Teams are used to search narrow and wide-body aircraft, vehicles, terminals, cargo warehouses, and luggage in the airport environment. TSA-certified teams are required to dedicate a pre-set portion of their daily activities to screening cargo being tendered for transportation on passenger aircraft and surveillance of air cargo facilities and aircraft operating areas. At designated locations, a TSA-certified team must screen all priority mail parcels of a minimum specified weight that are transported on passenger aircraft.

Objective 2: Increase the vigilance of travelers and transportation workers.

A number of programs directly support the objective of increasing the vigilance of travelers and transportation workers. For example, FAA supports several programs, including an identification (ID) media program for its personnel. It also conducts suitability investigations of employees and contractors, and carries out investigations of employees, non-employees, contractors, and airmen suspected of violating FAA orders and regulations. FAA provides investigative services for alleged criminal activity by airmen and other FAA certificate holders, use of unapproved aircraft parts, counterfeit certificates, falsification of

official documents, NAS security violations, property theft, and alleged employee misconduct and criminal activity. In addition, all commercial drivers associated with aviation services seeking a HAZMAT endorsement must undergo a Security Threat Assessment conducted by TSA's Office of Transportation Threat Assessment and Credentialing (TTAC).

Many commercial airline security regulations increase transportation worker vigilance through mandated reporting requirements and employee security training. While this increases vigilance among a broad group of people, passengers must also be aware of suspicious activity. Further development of vigilance and outreach programs continues to enhance awareness.

Since intelligence identifies aviation as a focus of terrorists, whether as a target or for use as a weapon, many current initiatives focus specifically on high-risk passengers. Certain technologies, such as biometrics, have emerged to securely identify those passengers traveling aboard aircraft:

- The **Registered Traveler** program has the potential to enhance security by biometrically identifying individuals who have completed favorable background checks, and may thereby expedite their screening process. This allows real-time screening to focus on other passengers using the aviation system who are not participating in the program. In addition to programs at the checkpoint, pre-screening enhancements continue to evolve to help identify passengers who pose the greatest risks to the aviation system. Also, the Secure Flight program is evaluating the transfer of the watch list vetting process from air carriers to the Federal Government in an effort to centralize vetting of all traveling passengers.
- In the **air cargo** arena, IACs and principal officials are being vetted through new automated systems, and background checks against Watch Lists are being conducted for all employees and contractors with unescorted access to air cargo. TSA's Known Shipper Management System collects and compares automated information against government and commercially available databases to validate shippers who are permitted to ship cargo aboard passenger aircraft.
- TSA develops and makes available to flight and cabin crewmembers an advanced self-defense training program that includes appropriate and effective responses for defending against an attacker. In the **Crew Member Self-Defense Training (CMSDT)** program, crewmembers receive and review a self-paced, interactive DVD and a student manual designed to familiarize them with basic self-defense concepts and techniques, and then attend a 1-day hands-on training session at a participating community college.
- TSA also implements the **Alien Flight Student Program**, which conducts security threat assessments on foreign students seeking certain types of flight training and mandates security awareness training for all flight instructors.

Objective 3: Enhance information and intelligence sharing among Transportation Systems Sector security partners.

While many security measures have been implemented or improved since the 9/11 terrorist attacks, TSA continues to work, in cooperation with all government and industry stakeholders, to identify and mitigate potential threats and risks. Given the vast size and dynamic nature of the industry, it is necessary to evolve with the changing threat environment. The airline industry's flexibility and its partnership with the Federal Government can provide the means to implement essential security measures and thwart terrorist attacks both now and in the future.

Intelligence sharing has made great progress since 9/11, and this collaboration must continue. Intelligence sharing, both within government and abroad, has been responsible for preventing attacks against aviation and other modes of transportation.

Every Federal Air Marshal is trained to report suspicious activities within the aviation domain. Federal Air Marshals file Incident Reports for all suspicious activities that a Federal Air Marshal believes require an interview with the person(s) engaged in the activity, and Surveillance Detection Reports for activities that, in the Federal Air Marshal's professional judgment, do not require an interview, but are suspicious in nature. Both of these raw reports, plus any suspicious incident reports submitted by airline employees and other individuals within the aviation domain are placed in the Tactical Information Sharing System (TISS) through a designated email address where they can be accessed and analyzed by FAMS and other law enforcement organizations. Airline employees are encouraged to send suspicious incident reports to FAMS through a designated email address. These

reports are also placed in the TISS database. In addition to TISS, there are a number of ongoing programs, such as Screening of Passengers by Observation (SPOT), that are intended to identify suspicious activities within the aviation domain.

TSA firmly believes that while prioritizing vulnerabilities and threats is a vital component in securing the Nation's Transportation Systems Sector, it is important to identify a broad spectrum of activities that could potentially be misused for terrorist purposes. Therefore, the agency continues to develop security guidance documents for GA airports, establish security protocols for corporate and fractional (group-owned) aircraft, and increase security awareness and vigilance using the **Airport Watch** program and the **1-866-GA-SECURE** hotline.

3.1.2 Goal 2: Enhance the Resiliency of the U.S. Transportation System

The objectives supporting sector goal 2 are:

- Manage and reduce the risk associated with key nodes, links, and flows within critical transportation systems to improve overall network survivability; and
- Ensure the capacity for rapid and flexible response and recovery to all-hazards events.

To continue to improve the aviation transportation system's risk profile, TSA, FAA, and other Federal security partners will focus on activities that not only manage risk, but also create resilience in the system, including activities focused on prevention and preparedness, as outlined below.

Objective 1: Manage and reduce the risk associated with key nodes, links, and flows within critical transportation systems to improve overall network survivability.

A number of key programs support the management and reduction of risk associated with key nodes, links, and flows within the aviation transportation system to improve overall network survivability.

The capacity for rapid and flexible response and recovery is also provided by TSA's **Transportation Security Operations Center (TSOC)**, a robust, fully operational operations center that is staffed 24/7 and comprised of three watches. One watch, the **Command Duty Officer (CDO)**, enables TSOC to provide communication and coordination, and establish domain and situational awareness across the entire transportation infrastructure. A goal of TSOC is to create a robust information-sharing environment by educating the TSA community and forming partnerships that promote fluid information exchange.

TSA is the Executive Agent for the second TSOC watch, the **National Capital Region Coordination Center (NCRCC)**. As such, it provides physical infrastructure and connectivity for other agencies, including North American Aerospace Defense Command, Northeast Air Defense Sector, FAA, FBI, U.S. Secret Service (USSS), U.S. Capitol Police, U.S. Customs and Border Protection, U.S. Coast Guard, and the Metropolitan Police Department (Washington, DC). NCRCC provides air space security for the national capital region, coordinates the activities of the participating agencies, actively reconciles conflicting procedures, and integrates the roles of each NCRCC representative.

The third TSOC watch is the **National Infrastructure Coordinating Center (NICC)**. As part of the DHS's Infrastructure Protection Division, NICC maintains operational awareness of the Nation's critical infrastructure and key resources (CI/KR). NICC provides a mechanism and process for information sharing and coordination between government and industry partners.

FAA efforts are targeted at improving overall network survivability, including the establishment of an interagency, real-time network called the **Domestic Events Network (DEN)**, which enhances shared situational awareness and coordinated decision-making on real-time security incidents involving NAS or otherwise affecting U.S. interests. DEN is an unclassified telephonic conference among air traffic control facilities, military entities, government agencies, and law enforcement officials that allows real-time information to be shared simultaneously among all entities responsible for analyzing and responding to significant aviation events. The Command, Control, and Communications (C3) program provides the engineering, implementation, and

maintenance support for FAA systems, which include the VHF/FM radio installations at nearly 900 locations nationwide and the fixed satellite installations at more than 100 airports and air traffic control facilities.

FAA also employs an integrated system of policy, procedures, personnel, facilities, and communications that ensures that aviation officials have timely, accurate information to plan, direct, and control all aspects of FAA-essential operations and functions during emergency situations. FAA plans, directs, and manages its essential operations during emergencies through established emergency operations programs. These established programs include disaster management, pandemic influenza planning, C3, continuity of operations (COOP), and emergency-related exercises. FAA provides guidance and assistance to all lines of business, staff offices, and field elements.

FAA maintains continuous command, control, and communications with its field elements, other government agencies, and the aviation industry to ensure that aviation officials have immediate access to information. This is critical to managing events that have an impact on NAS, including natural disasters and Incidents of National Significance.

Finally, FAA designs and implements air traffic and airspace management-related security measures in concert with its partners, including air traffic control intervention, using Temporary Flight Restrictions (TFRs) to protect sensitive targets, monitoring NAS operations, and participating in specialized security interagency mechanisms such as Man-Portable Air Defense System (MANPADS) Mitigation Plans.

Objective 2: Ensure the capacity for rapid and flexible response and recovery to all-hazards events.

Ensuring that essential functions continue contributes to the resiliency of the transportation system. As a baseline of preparedness for the full range of potential emergencies, all Federal agencies are required to have in place a viable COOP capability, which ensures the performance of their essential functions during any emergency or situation that may disrupt normal operations. For example, in a catastrophic event, FAA support personnel would be deployed to a best response location. In a hurricane, for instance, personnel would be deployed to provide local communications support to responders. During an influenza pandemic, minimal support staff would be provided at critical locations and other support would be provided remotely. A terrorist event would probably result in full staffing of all specialties to support all affected locations for the duration of the event.

TSA's **Emergency Preparedness Division (EPD)** is also located at TSOC. EPD represents TSA in preparing, planning, and conducting exercises at all levels—from internal tabletop to national-level multi-agency events—simulating incidents requiring a response based on policies and procedures established for the entity involved. EPD also manages an After Action Report program to identify weaknesses and issues identified from exercises, assign offices to be responsible for correcting the reason for the problem, and track these assignments to ensure completion.

An ongoing TSA effort that will help ensure the capacity for rapid and flexible response and recovery to all-hazards events is the **Natural Disaster Preparedness Plan (NDPP)**, currently under development. NDPP will ensure continued aviation transportation system security and facilitate support for other Federal, State, and local emergency response operations in areas affected by disasters, while meeting the needs of TSA employees (e.g., allowing them to prepare their homes and evacuate their families). NDPP facilitates planning, preparation, and resource allocation for Headquarters personnel, Federal Security Directors and staff, and disaster support teams that will respond to assist affected TSA operations. These response teams are trained, equipped, and exercised, making them ready to rapidly deploy in the event of a natural disaster.

3.1.3 Goal 3: Improve the Cost-Effective Use of Resources for Transportation Security

The objectives supporting sector goal 3 are:

- Align sector resources with the highest priority transportation security risks using both risk and economic analyses as decision criteria;
- Ensure robust sector participation as a partner in developing and implementing public sector programs for CI/KR protection;

- Improve coordination and risk-based prioritization of Transportation Systems Sector security research, development, test, and evaluation efforts; and
- Align risk analysis methodologies with the Risk Analysis and Management for Critical Asset Protection (RAMCAP) criteria outlined in the NIPP.

Objective 1: Align sector resources with the highest priority transportation security risks using both risk and economic analyses as decision criteria.

While the overall Transportation Systems Sector SBRM methodology has been developed, specific implementation programs and tools are still evolving. The SBRM methodology detailed in the Transportation Systems SSP contains a series of steps that must be completed to identify a comprehensive portfolio of mitigation options and countermeasures. Criteria for selecting the aviation mode's critical systems, as well as the mode's critical assets, must first be established to define the scope of risk management activities. These screening criteria will define what is "critical" within the mode. Once the systems and assets have been screened, the means to conduct vulnerability assessments, including physical, process, and institutional components, must also be defined. It is likely that a variety of tools and methodologies will need to be integrated to support the differences between systems and assets, as well as differences between asset types. The resulting prioritized portfolio of risk mitigation activities will be informed and updated based on the relevant risks to the mode.

TSA monitors the flight activities of thousands of **Federal Flight Deck Officers (FFDO)** flying U.S. commercial passenger and cargo aircraft. Under the Arming Pilots Against Terrorism Act, TSA established a program to deputize eligible volunteer pilots of commercial passenger aircraft as Federal law enforcement officers to defend the flight decks of their aircraft with force, including deadly force, against acts of criminal violence and air piracy. The FFDO program was subsequently expanded to include pilots of all-cargo aircraft, flight engineers, and navigators.

TSA's **Armed Security Officer (ASO)** program enables eligible persons with sufficient law enforcement experience to provide armed security aboard GA aircraft authorized to operate into and out of Ronald Reagan Washington National Airport (DCA). TSA established security procedures that allow certain GA operations to resume at DCA, while protecting critical national assets from possible airborne terrorist attack. These procedures include a requirement that each GA flight operating into or out of DCA have onboard an ASO specially trained and authorized by TSA.

Each day hundreds of armed Federal law enforcement agents fly armed on domestic flights. The **Force Multiplier Program** could allow TSOC to track the movement of individuals from participating organizations, and provide situational awareness of law enforcement aboard an aircraft in the event of an incident.

Objective 2: Ensure robust sector participation as a partner in developing and implementing public sector programs for CI/KR protection.

The aviation industry bears significant costs associated with implementing security measures. The Federal Government recognizes the need to integrate analysis of increased security measures with the safety and efficiency needs of the aviation transportation system. Thus, the Federal Government must constantly evaluate the burden placed on the industry, while it addresses the current threat environment. Through the partnership already established between government and industry, changes to the security realm are almost always the result of consultation with aviation stakeholders. Through these discussions, government resources align with those in the industry to alleviate unnecessary costs and promote further security enhancements. It is critical that the Federal Government continues this ongoing partnership so that future threats may be successfully mitigated while applying rational security developments. Working together in these partnerships will facilitate the systematic review of lessons learned so that cost-effective, but resilient, security measures are implemented in the future.

Objective 3: Improve coordination and risk-based prioritization of Transportation Systems Sector security research, development, test, and evaluation efforts.

Research and development (R&D) has always been essential to the Transportation Systems Sector and represents a primary strategy to deter and prevent terrorist actions. Ongoing challenges to sector R&D efforts include the diversity of ownership of Transportation Systems Sector assets, the inherent vulnerability of aviation and surface transportation, the constant evolution of transportation security, and the increasing dependency on intermodal and international transportation. For these reasons, continual involvement by the private sector and Transportation Systems Sector stakeholders is paramount to successfully address these challenges.

TSA's risk assessment framework will be used to identify and prioritize critical systems and assets. Once the risks are identified, the areas of concern will be verified with appropriate government and stakeholder participants. Risk mitigation options, including physical, process, and institutional changes, will be considered for these systems and assets. Assessing the options based on their alignment with Transportation Systems Sector security goals, R&D strategic goals and other guidance from sector stakeholders will provide a prioritization of the mitigation options.

R&D requirements are derived using a technology scan approach of available options to be considered, including current best practices. From these requirements, development efforts are derived, often including identification of short-, medium-, and long-term desired outcomes. If approved, the path results in either basic, applied, or development research program(s) or some combination thereof. These programs may then result in pilot test programs in appropriate laboratories, followed by deployment or testing in the field.

The Federal Government is introducing new pilot programs that integrate and coordinate various measures. For example, the great variety and composition of items to be inspected in air cargo pose a very different challenge from that of inspecting baggage. Pilot programs designed to identify innovative methods to protect the integrity of air cargo from the time of acceptance until tendering at the airport will evaluate tamper-evident and tamper-resistant seals and locks to secure air cargo in transit. To determine an optimal array of security measures, other programs will evaluate the effectiveness of canines to inspect a higher percentage of air cargo in various configurations, as well as to determine the efficiency, effectiveness, and operational impact of other technologies. 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.

Since Transportation Systems Sector 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. Many of these requirements will be addressed through normal planning and programming activities. If the capability does not currently exist, an examination of other programs will be conducted that may be adapted to address the need or direct new R&D activities through the grants process or other funding vehicles to encourage new design capabilities.

R&D inputs to requirements are also driven by the evolution of technology capabilities. The continual scanning for new technology 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.

Objective 4: Align risk analysis methodologies with the RAMCAP criteria outlined in the NIPP.

RAMCAP will be the primary tool used to assess risk at the asset level. RAMCAP process steps establish common criteria for conducting strategic risk analyses that can be applied across all 17 CI/KR sectors. Common criteria include using common terminology and reporting for defining Asset and Threat Characterization; Consequence Analysis; Vulnerability Analysis; Threat and Risk Assessment; and Risk Management. RAMCAP also provides a common, non-sector-specific reporting framework that

can be used to normalize and compare assets from different sectors, enabling informed resource allocation and consequence mitigation decisions around the Nation's CI/KR.

The DHS is currently using RAMCAP in the Nuclear Reactors, Materials, and Waste Sector and piloting the tool in the Chemical Sector. Other sector module sets, such as transportation, will follow. The Transportation Systems Sector will work with the appropriate organizational elements of the DHS and the American Society of Mechanical Engineers to coordinate creating a RAMCAP version for the Transportation Systems Sector. This effort will document guidance on approaches and methodologies for analyzing risks to assets associated with adversary attacks, identifying and developing countermeasures and consequence mitigation strategies to reduce risks, and evaluating countermeasures and consequence mitigation strategies using cost-benefit analyses and other methods to inform resource allocation decisions.

Once transportation modules have been created, RAMCAP results will allow the Transportation Systems Sector to work directly with the DHS and other Federal agencies to prioritize countermeasures for various assets from different sectors based on comparative risk analyses. This will, in turn, allow the DHS and other agencies to implement security measures that employ the Nation's resources for maximum security. Until RAMCAP modules for the Transportation Systems Sector are developed, facilitated assessments may rely more heavily on current transportation modules already defined and in use.

3.2 Effective Practices, Security Guidelines, Requirements, and Compliance and Assessment Processes

The initiatives outlined below represent a large body of aviation mode-specific plans that address the full range of aviation transportation system security issues and are discussed in relation to their direct correlation to the goals and objectives previously mentioned in section 3.1. A listing of programs related to these plans can be found in appendix 1, which lists aviation programs organized by sector.

3.2.1 Industry Effective Practices

Industry effective practices are security measures or processes that private industry recognizes (but the Federal Government does not formally require) as performance standards. They may cover a wide range of security areas, including risk assessments, employee screening, access controls, intrusion detection, IT security, awareness training, incident management, and exercises.

3.2.2 Security Guidelines

Security guidelines are any formal security-related guidance that the Secretary of Homeland Security recommends, for implementation on a voluntary basis, to enhance the security of a transportation system.

Common Strategy #2. TSA and FAA developed the current version of the Common Strategy in coordination with the FBI, the airlines, and other key stakeholders following the 9/11 attacks to provide updated, consistent guidance to aircrews on how to best handle a hijacking situation. This guidance, which is integrated into TSA's Aircraft Operator Standard Security Program (AOSSP) and other programs addressing the user community, established a new strategy designed to deal with terrorist hijackers who intend to cause mass casualties, in contrast with the conventional hijacker, whose motive might be ransom, escape from the law, political asylum, or publicity. Common Strategy #2, which was originally implemented on January 18, 2002, addresses the use of plain language in controller-pilot communications, the critical need to defend the cockpit, and the use of special transponder codes. TSA, FAA, and their partners are continuing to refine and enhance the implementation of Common Strategy #2.

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 to the commercial airport industry, providing security guidance on airport layout, security screening, emergency response, access control and communications, and other topics. This document is intended for professionals in the engineering, architecture, design, and construction fields. A

team composed of 10 government agencies and approximately 135 private sector experts in a wide variety of security, aviation, and architectural disciplines worked together for 18 months to produce this document.

General Aviation Airport Security Guidelines Information Publication (IP). In May 2004, the DHS/TSA, in cooperation with the GA industry, developed an IP entitled General Aviation Airport Security Guidelines. The IP acts as a set of best practices/guidelines and is a guidance document for individuals with oversight responsibility of GA airports and facilities. The IP offers recommended security measures that can be applied to GA airports regardless of size and type of operation, and will offer potential solutions to airports that presently want additional security enhancements. Furthermore, the IP is available on the DHS/TSA Web site, www.tsa.gov/assets/pdf/security_guidelines_for_general_aviation_airports.pdf; TSA encourages State, county, and local officials to use it to assess their respective GA airports.

Airport Watch/1-866-GA-SECURE. The main security focus for recreational flying has centered on enhancing security at GA airports where the bulk of these operations occur. TSA, in partnership with the Aircraft Owners and Pilots Association (AOPA), implemented the Airport Watch program, which increases the security vigilance of the flying public and directs industry to contact the toll-free national government hotline (operated by TSA/TSOC) to report suspicious activities. This program provides a mechanism for any GA pilot or airport employee to report suspicious activities to a central Federal Government focal point.

3.2.3 Security Requirements

Security requirements are regulatory actions, including security directives, when necessary and appropriate, to implement measures to enhance the security of a transportation system.

Sensitive Security Information. 49 CFR 15 and 1520, Protection of Sensitive Security Information, are regulations that regulate the release of various records and information, including those obtained or developed during particular security activities.

Security Regulations/Programs. For commercial aviation, 49 CFR 1544 describes all required security measures for aircraft operators and outlines the various security programs that particular aircraft operators must use, depending on the operation. Six unique programs are outlined in section 1544: (1) full, (2) private charter, (3) twelve-five, (4) partial, (5) all-cargo, and (6) limited programs. Unlike the passenger and baggage screening procedures performed by TSA, these measures generally do not take place within public view and are almost always performed by aircraft operators. Some of the procedures that each carrier is responsible for performing-depending on the program-include vetting passengers against TSA No-Fly and Selectee Lists, searching the interior and exterior of aircraft, screening and securing cargo, and developing a security training program for crewmembers.

Airport Security Program (ASP). 49 CFR 1542 provides baseline security requirements for defined types of commercial airports. Under the regulation, airport operators must adopt and comply with an ASP. Once the airport operator develops the ASP, the Federal Security Director (FSD) must review and approve it. When approved, the ASP becomes the vehicle by which TSA can inspect and enforce security measures. An authorized Airport Security Coordinator (ASC) has custodial responsibility for the ASP and must inform TSA of any proposed changes to it.

Security Directives (SDs) and Emergency Amendments (EAs). Because of the ever-changing risks to commercial aviation, government and industry stakeholders, IACs, and foreign carriers must proactively develop new procedures to mitigate threats or address security loopholes. Based on specific intelligence information or other appropriate circumstances, the government issues SDs/EAs to make rapid security adjustments. SDs/EAs require aircraft and airport operators to implement new security procedures, often on short notice. SDs are developed to mitigate certain threats, provide security measures for travel to specified airports, and develop adjusted procedures for changes in the homeland security threat level.

Security Advisory. On a continuous basis, TSA uses a threat-based, risk management, and consequence-based approach, including analyzing intelligence information, to monitor the security environment surrounding commercial aviation operations and assets, as well as those of GA. TSA will develop and disseminate a Security Advisory in the event that a situation arises that requires increased scrutiny and vigilance by the American public. These advisories are given widespread dissemination through

the cooperation of aviation industry associations and Federal, State, and local authorities. A Security Advisory is a summary of relevant and timely facts on GA security that is meant to increase security awareness.

MANPADS Vulnerability Assessments (MVAs)/MANPADS Mitigation Plans (MMPs). TSA, in cooperation with the FAA; airport operators; Federal, State, and local law enforcement; and other key stakeholders, has conducted MVAs at more than 300 airports around the country. [LMB1]These MVAs have been used to establish airport-specific MMPs, which the local FSD, in consultation with the aforementioned partners, exercises, updates, and manages. In accordance with national-level MANPADS guidance, the MMPs establish the roles and responsibilities of the various stakeholders, notification procedures, countermeasures (e.g., strategic deployment of law enforcement assets to probable launch areas), and crisis response processes. TSA; FAA; Federal, State, and local agencies; and their partners are continuing to refine and strengthen these MMPs.[LMB2]

Twelve-Five Standard Security Program (TFSSP). This program provides security requirements for charter operators in aircraft with a maximum takeoff weight greater than 12,500 pounds operating under 14 CFR 135. For example, the program requires that pilots be vetted through the TSA security program and passengers be checked against the No-Fly List.

Restoration of General Aviation at Ronald Reagan Washington National Airport (GA@DCA). This program permits the reutilization of DCA by certain GA aircraft that apply for and comply with the regulation and program. The program requires that crewmembers be vetted, passengers be checked against the No-Fly List, an armed security officer fly with passengers into/out of DCA, all crewmembers and passengers and carry-on baggage be screened, and TSA inspect the aircraft prior to departure. Additionally, the rule requires fixed-base operators (FBOs) to comply with the FBO standard security program.

Maryland Three Rule (MD-3). This program authorizes the operation of three Maryland GA 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.

3.2.4 Compliance and Assessment Processes

Compliance and assessment processes are methods used to measure compliance against effective practices, security guidelines, or security requirements. Compliance and assessment processes can take the form of regulatory inspections, voluntary inspections, risk assessments, data calls, or other methods.

Compliance and Assessments. The TSA Office of Compliance is responsible for enforcing aviation security regulations and programs. TSA employs hundreds of Aviation Security Inspectors (ASIs) at airports across the United States to conduct compliance inspections of air carriers and work with regulated entities to help correct identified security deficiencies. Each aircraft operator is also assigned a Principal Security Inspector (PSI) to ensure overall security compliance at the corporate level. TSA deploys aviation security personnel to assess foreign airports, from which U.S. and foreign air carriers operate to the United States, for compliance with the security standards of the International Convention on Civil Aviation (Chicago Convention). 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 the foreign government authorities of that decision and recommends steps to achieve compliance. If the airport fails to comply within 90 days of such notice, the 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. and foreign air carriers providing transportation to the airport from the United States must provide written notice to passengers of the decision on or with the ticket sold for flights to that airport. 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 from a point in the United States.

In addition, TSA inspects foreign air carrier stations from which flights operate to the United States, as well as all U.S. air carrier stations located overseas. TSA deploys inspectors to specified foreign locations when the threat level indicates the need for their presence. PSIs are assigned to liaise with foreign air carriers and all-cargo aircraft operators. The PSIs are part of the TSA International Programs Office Foreign Air Carrier Security Program. Under the Foreign Airport Assessment Program and Air

Carrier Inspection Program, the International Programs Office 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.

The International Programs Office is responsible for liaison with foreign air 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. In fiscal year (FY) 2004, the International Programs Office conducted more than 550 air carrier inspections of foreign and U.S. air carriers at foreign airports. Legislation for this program will require that all FAA-certificated Part 145 repair stations be subject to security regulations. It will further require all foreign repair stations to undergo a security review and audit. TSA is developing the Foreign Repair Station Program to ensure the security of maintenance and repair work conducted on U.S. air carrier aircraft and components at domestic and foreign repair stations, as required in 49 United States Code (U.S.C.) 44924.

Crew Vetting Program (CVP). TSA's Office of Transportation Threat Assessment and Credentialing (TTAC) administers the CVP, which vets foreign and domestic aircrews flying internationally into, out of, and over the United States against terrorism watch lists.

Alien Flight Student Program (AFSP). AFSP requires that foreign flight students who plan to participate in certain types of flight training submit information for a security threat assessment before commencing that training. The rule and program also require flight training providers to register with TSA and participate in security awareness training. Additionally, the program enables TSA inspectors to inspect all flight training providers.

Facility Security Management Program (FSMP). The FAA 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 assessments and inspections to determine compliance with facility security, communications, security, classified information, national directives, and DOT policies that influence FAA security practices.

3.3 Grant Programs

The DHS has several security grant programs and TSA provides technical assistance in evaluating grant proposals. TSA also provides technical evaluations during the processing of FAA Airport Improvement Program (AIP) grants. FAA's AIP provides grants to public agencies-and, in some cases, to private owners and entities-for planning and developing public-use airports that are included in the National Plan of Integrated Airport Systems (NPIAS). NPIAS identifies public-use airports that are important to public transportation and contribute to the needs of civil aviation, national defense, and the U.S. Postal Service. Eligible projects include those improvements related to enhancing airport safety, capacity, security, and environmental concerns. In general, sponsors can use AIP funds on most airfield capital improvements or repairs except those for terminals, hangars, and non-aviation development.

Risk assessment for AIP funding occurs on both the national and local levels. Because the demand for AIP funds exceeds the availability, FAA bases distribution of these funds on present national priorities and objectives. AIP funds are typically first apportioned into major entitlement categories such as primary, cargo, and general aviation. Remaining funds are distributed to a discretionary fund. On the local level, independent risk assessment studies are conducted at airports requesting AIP funds, with their nature related directly to the needs of the particular airport. 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 are two interwoven development categories under NPIAS. They include development that Federal regulation, airport certification procedures, or design standards require, and are intended primarily to protect human life. These two categories, which combined account for 5 percent of the funding needs identified in the NPIAS, include obstruction lighting and removal, fire and rescue equipment, fencing, and security devices. Safety development totals an increase of 23

percent from 2001 to 2005, while security costs total an increase of 69 percent in the same period. This increase reflects the costs associated with improving runway safety areas, as well as the costs associated with modifying terminals to accommodate explosive detection systems and other security enhancements. 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.

3.4 The Way Forward

The Federal Government responded to the attacks of 9/11 with a comprehensive increase in measures to enhance aviation security. Significant improvements were made to existing security methodologies, operations, and technologies through creating systems of security in each area of the aviation transportation system. The Federal Government established a scalable, flexible aviation security system that is responsive to varying threat levels and to the range of current and future threats to the United States and effectively reduced vulnerabilities within the aviation transportation system. Significant enhancements were made in the ability to detect threat objects and explosives that could be brought on or otherwise used against aircraft, and increases in the security posture of the entire air domain were made.

Collectively, these security measures have created multiple barriers, greatly reducing the likelihood of a successful attack. These measures represent important steps forward; however, no individual component is totally fail-safe. Moreover, terrorists are continuing to devise methods for defeating security efforts, as evidenced by the recent threats to U.S.-bound flights identified by officials in the United Kingdom.

The ever-changing threat environment in the aviation transportation system provides numerous challenges to the Federal Government and private industry for implementing effective and efficient security measures. To continue addressing the persistent threat, government and its aviation stakeholders must cooperate in developing a layered security system through established programs and innovative enhancements.

Looking forward, the Federal Government, in coordination with its industry partners, will evaluate the need to amend aviation security programs to address potential vulnerabilities and gaps. In addition, employee security training programs will continue to evolve for the increased protection of passengers and aircraft, with a special emphasis on vigilance and suspicious activity detection.

The Federal Government, in coordination with stakeholders, will continue to communicate security changes and threat information to educate the traveling public. Improved intelligence will assist with these efforts as information sharing increases among all Federal agencies. Intelligence sharing must continue to be enhanced to ensure that threats to the aviation system are constantly in focus. It is critical that aviation stakeholders remain educated and flexible to adapt to any changes in security procedures and to ensure that new procedures are instituted quickly and accurately. Likewise, the Federal Government must continue to be proactive, but prudent, to ensure that any strengthened measures do not place unnecessary burdens on the industry.

Looking to the future, several government initiatives intersect around aviation security. In particular, two organizations are joining forces to plot the way forward to the airport of the future, in which security measures will result in minimal adverse operational impacts, while focusing scarce resources on vulnerabilities identified through a risk-vulnerability-consequence review. These organizations are the Security Identification Display Area II (SIDA II) Work Group within TSA, and the Security Integrated Product Team (SIPT) of the Joint Planning and Development Office (JPDO).

The mission of SIDA II is to review and, where necessary, redesign the current state of those security requirements applied in separating the public (land side) from the non-public (air side) portions of airports. Under SIDA II, the main areas currently under review are Background Checks and Access Authority, Perimeter Access Controls, and Airside Response and Surveillance.

JPDO was established in 2003. Its mission is to transform the U.S. aviation landscape from the current state to that of 2025 and beyond. The vision is to accommodate an anticipated threefold 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, JPDO will work cooperatively with SIDA II to leverage resources and shared visions to design and implement a security infrastructure that will ensure a robust and secure aviation environment.

FAA's Next Generation Air Transportation System (NextGen or NGATS) initiative is a complete air traffic system redesign to enable FAA to reduce delays, improve aircraft management, and maximize safety and efficiency. FAA is working with the National Aeronautics and Space Administration (NASA), the DHS, DoD, and the Department of Commerce to expand the NGATS initiative beyond capacity to include security and national defense. The U.S. Air Force and FAA are working together, for example, on how to accommodate the growing numbers of unmanned aerial systems. FAA has included several stakeholders in this initiative, including State and local governments; the Aerospace States Association, made up of lieutenant governors and governor-appointed delegates; and private sector stakeholders.

Numerous government and industry studies have identified potential areas of improvement in the security of the air cargo system. TSA and its partners are forming a number of initiatives that they believe will meet future challenges in ensuring the security of air cargo. Long-term improvement efforts have been implemented, including development of comprehensive cargo security programs and incentive-based programs. Some of these programs can be found in appendix 1 of this document.

The sheer volume of air cargo, combined with current technology limitations, makes inspecting all air cargo challenging. The flow of commerce is similar to an airline hub-and-spoke system with thousands of input lines feeding into a relatively few number of system access points. The combination of diversity of ownership and decentralization of access control associated with this supply system creates a unique challenge to anticipate, coordinate, and plan for air cargo security concerns from origin to destination. This curb-to-cargo-hold challenge will be a focus area of future R&D programs.

Because of the wide variety and scope of GA aircraft and landing locations, any approach to implementing security guidelines must consider the various types of flight operations, as well as the size of aircraft involved, among other factors. Therefore, a flexible, common-sense approach to GA airport security is important if the industry is to retain its economic vitality.

For GA, TSA will continue to use a threat-based, risk management, and consequence analysis approach to analyzing and prioritizing the vulnerabilities and threats to GA assets and conveyances. This approach includes the continuous review of existing security programs and policies to align security measures with vulnerabilities and threats, reduce security loopholes, and implement reasonable/feasible security requirements that maintain an appropriate level of security. As intelligence information and vulnerabilities in the GA system are identified, TSA will modify existing programs and develop new programs and policies to address the threat.

3.5 Metrics

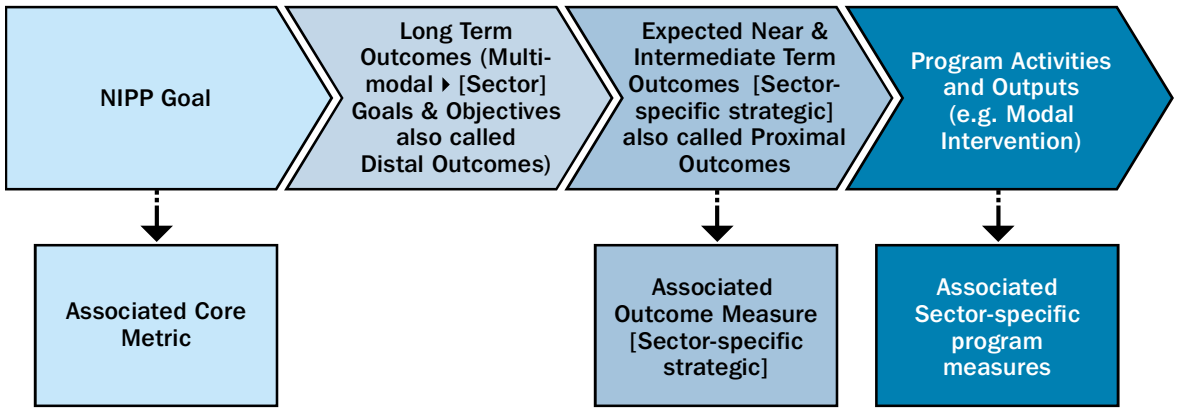
General. To evaluate the collective impact of the Transportation Systems Sector's efforts to mitigate the risks to the transportation infrastructure and to increase the resilience of the transportation system through information-sharing mechanisms, measures of effectiveness must be developed and monitored. Metrics that are developed will supply the data either to affirm that Transportation Systems SSP goals are being met or to show what corrective actions may be required. This section is an overview of the plan to implement a Transportation Systems SSP measurement program. To be effective, the measurement program will require the cooperation of all modal GCCs and SCCs to provide accurate responses to the metrics being used to measure sector risk posture, Transportation Systems SSP effectiveness in the sector, and security program effectiveness.

Measurement Joint Working Group. A Measurement Joint Working Group will be formed under the Transportation Systems Sector GCC/SCC and will be comprised of one member from each modal GCC and SCC or their designate and invited measurement professionals. Under the leadership of TSA's lead measurement organization, the group will operationalize measures; establish data sources, data collection, and verification procedures; set measurement policy for the Transportation Systems SSP; and approve supporting procedures. The group may also require standardization of certain measurement practices from data

contributors across the sector. The Measurement Joint Working Group will communicate regularly with Transportation Systems Sector GCC/SCC members to ensure that working group progress and plans are fully transparent and coordinated with the members. In addition, the work products of the Measurement Joint Working Group will be submitted, when appropriate, to the overarching Transportation Systems Sector GCC/SCC for approval.

Measures. The Outcome Monitoring methodology, as exemplified in figure A3-1, demonstrates working down from the national and multi-modal (sector) goals to determine outcomes and their respective measures.

Figure Annex A3-1: Outcome Model



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

1. **Core.** Core NIPP metrics are common across all sectors and focus on measuring risk-reduction progress in the sector. These measures are often descriptive statistics (counts). For example: Percentage of medium- and high-consequence assets with completed vulnerability analyses.

2. **Sector-Specific Strategic.** These metrics are used to gauge the overall effectiveness of the sector toward meeting Transportation Systems SSP goals and objectives. Ordinarily, these are outcome measures capable of quantifying the degree to which the Transportation Systems SSP is having an effect on sector security. In the early stages of the program, proxy or substitute output measures may need to serve as proxies for the long-term outcome measures. In this instance, output data are likely to be collected from each mode and combined at the sector level (or reported independently at the mode level). For example: Goal 1, Objective 1 states, Implement flexible, layered, and unpredictable security programs using risk management principles. The measurement objective is: Risk-based, flexible, layered, and unpredictable security programs. A near- and intermediate-term outcome for aviation might be: Risk-based, unpredictable security programs. An example outcome measure then might be: Effectiveness of unpredictable security programs.

3. **Sector-Specific Program.** These measures are aligned to the strategic risk objectives (i.e., priorities, strategies) for the Transportation Systems Sector. The strategic risk objectives for the sector will be developed according to the discussion in section 3 of the Transportation Systems SSP Base Plan. Strategic risk objectives are developed with program measures and should be aligned to the overall Transportation Systems SSP goals and objectives. Standard performance measurement techniques for programs will be supplemented with measures to demonstrate how the program is meeting associated Transportation Systems SSP strategic risk objectives.

4 Program Management

The Transportation Systems SSP Base Plan presents an approach for the aviation mode to capture, comprehend, and explain the relationship between setting priorities (What are we concerned about?), developing programs (What are we going to do about it?), and understanding current capabilities (What are we doing now?) to set a clear direction for risk management efforts. The goal of this approach is a scalable and agile multi-stakeholder security system that makes the most of scarce resources to protect the Nation's critical aviation transportation system infrastructure in a complex and constantly evolving environment.

The Transportation Systems SSP Base Plan points out that planning, or gaining an understanding of how business is being done today in the aviation mode (the "as is" state), is a key first step to determining where the mode needs to be in the future (the "to be" state). The second step is programming, or implementing an effective balance of programs while avoiding unnecessary duplication of efforts and also preventing dangerous gaps. Finally, in the budgeting phase, lead Federal partners will provide detailed budget justifications and program execution plans.

As noted in the Base Plan, the maintenance of security programs-and their continued contribution to the sector's resilience strategy-is a shared responsibility. The Federal partner is responsible for the planning, programming, and budgeting steps, and will maintain federally operated programs. The Federal partner will also be responsible for providing standardized feedback and conducting an annual survey on the effectiveness and efficiency of its programs. This feedback will be used to guide program sustainment or adjustment and to collect best practices and lessons learned in developing new programs.

The success of any aviation transportation system security program is based, in large part, on the input and cooperation of relevant stakeholders. Coordination and communication with stakeholders is vital to ensure that any changes in Federal program execution (including termination) that will impact other programs or planning efforts at any level are properly explained and efficiently carried out.

As described earlier in this annex (section 2.3), the Secretary of Homeland Security exercised his authority to create a committee to facilitate public-private consultation on matters of critical infrastructure protection. Under this umbrella authority, several committees have been formed to focus on protecting critical infrastructure in the Transportation Systems Sector of the national economy, including the Transportation Systems Sector GCC.

Appendix 1: Matrix of Aviation Programs

Program	Responsible Agency	Goal(s) 1, 2, 3
Cross-Modal Programs		
Transportation Security Lessons Learned Information Sharing (LLIS)	DHS/TSA	1, 3
Homeland Security Advisory System (HSAS)	DHS	1
Continuity-of-Operations Program (COOP)	DHS/ALL	1, 2
Visible Intermodal Protection and Response (VIPR)	TSA	1, 2
Customs-Trade Partnership Against Terrorism (C-TPAT)	CBP/TSA	1, 3

Program	Responsible Agency	Goal(s) 1, 2, 3
National Explosive Detection Canine Team Program (NEDCTP) Rapid Deployment Canine Team Force (NRDCTF)	TSA	1
National Capital Region Coordination Center (NCRCC)	TSA	1, 2
National Infrastructure Coordination Center (NICC)	TSA	1, 2, 3
Transportation Security Operations Center (TSOC)	TSA	1, 2
Transportation Worker Identification Credential (TWIC)	TSA	1
NAS Infrastructure: Fixed Assets		
FAA Information Security Systems (ISS)	FAA	1, 2, 3
Facility Security Management Program	FAA	1
Visitor Vetting and Control	FAA	1
Mail and Delivery Screening	FAA	1
NAS Infrastructure: Human Capital		
HSPD-12 Joint Program Office Initiatives	FAA	1, 3
Personnel Security	FAA	1
Air Carrier/In-Flight Security Programs		
Air Traffic Security Coordinator (ATSC)/Air Defense Liaisons (ADLs)	FAA/TSA	1
Aviation Worker Background Check Program (AWBCP)	TSA	1
Domestic Events Network (DEN)	FAA/TSA	1, 2
Federal Air Marshal Service (FAMS) Mission Deployments	TSA	1, 3
FAMS Force Multiplier (FAMSFM) Program		
Federal Flight Deck Officer (FFDO) Program	TSA	1
National Capital Region Coordination Center (NCRCC)	TSA	1, 2
Registered Traveler	TSA	1
Secure Flight Program	TSA	1

Program	Responsible Agency	Goal(s) 1, 2, 3
Temporary Flight Restrictions	FAA, TSA	1, 2
Tactical Information Sharing System	TSA	1
Aircraft Operator Standard Security Program	TSA	1
Airport Security Programs		
Aircraft Operator or Foreign Air Carrier Exclusive Area Agreements	TSA	1
Airport Security Area Screening (Aviation and Transportation Security Act (ATSA) Section 106)	TSA	1
Airport Security Consortia (Local Advisory Committee)	TSA	1
Airport Security Officer (ASO) Program	TSA	1
Airport Tenant Security Program (ATSP)	TSA	1
Homeland Security Advisory Threat Condition Enhancements (Aviation Security (AVSEC) Levels)	TSA	1
Improved Airport Perimeter Access Security (Aviation and Transportation Security Act (ATSA) Section 106)	TSA	1
Investigative and Enforcement Procedures	TSA	1
U.S. Airport Emergency Plan (AEP)	TSA	1, 2
U.S. Airport Inspection Program (Annual Work Plan)	TSA	1
U.S. Airport Security Program (ASP)	TSA	1
U.S. Airports Voluntary Security Construction Guidelines	TSA	1, 3
Vendor Security Program	TSA	1
Airport Checkpoint Operations		
Backscatter	TSA	1
Document Scanners	TSA	1
Explosives Trace Detection (ETD) (Checkpoint Operations)	TSA	1
Handheld Metal Detectors (HHMDs)	TSA	1
Screening of Passengers by Observation Techniques (SPOT) Program	TSA	1
Secondary Screening (Checkpoint Operations)	TSA	1

Program	Responsible Agency	Goal(s) 1, 2, 3
Threat Image Projection (TIP) Ready X-Ray (TRX)	TSA	1
Trace Portal	TSA	1
Walk-Through Metal Detectors (WTMDs)	TSA	1
Airport Checked Baggage Operations		
Approved Alternative Screening Procedures (Checked Baggage Operations)	TSA	1
Explosives Detection Systems (EDS) (Checked Baggage Operations)	TSA	1
Explosives Trace Detection Equipment (Checked Baggage Operations)	TSA	1
Secondary Screening (Checked Baggage Operations)	TSA	1
Air Cargo Inspections		
Air Cargo Freight Assessment System	TSA	1
Air Cargo Surveillance Program	TSA	1
Full All-Cargo Aircraft Operator Standard Security Program (FACAOSSP)	TSA	1
Indirect Air Carrier (IAC) Revalidation Project	TSA	1
TSA Known Shipper Database Project	TSA	1, 3
General Aviation		
Airport Watch and 1-866-GA-SECURE Hotline	TSA	1, 2
Alien Flight Student Program	TSA	1
General Aviation at Ronald Reagan Washington National Airport (GA@DCA)	TSA	1
Information Publication: “Security Guidelines for GA Airports”	TSA	1
Maryland Three (MD-3) Airport Inspection Program	TSA	1
Restoration of General Aviation Access to Ronald Reagan Washington National Airport (GA@DCA)	TSA	1
Private Charter Standard Security Program	TSA	1
Transportation Security Administration Access Certificate: TSAAC Protocol	TSA	1
Twelve-Five Standard Security Program	TSA	1

Program	Responsible Agency	Goal(s) 1, 2, 3
International Programs		
Aircraft Repair Station Program	FAA/TSA	1
Foreign Air Carrier Model Security Program	TSA	1
Foreign Airport Assessment and Air Carrier Inspection Program and Automated Foreign Airport Assessment Program	FAA/TSA	1
Overseas Air Carrier Station Inspection Program	TSA	1
Counter Improvised Explosive Devices (IEDs)		
Bomb Appraisal Officer (BAO)	TSA	1
Threat Containment Unit (TCU)	TSA	1
Counter Man-Portable Air Defense Systems		
Counter Man-Portable Air Defense Systems (MANPADS) Vulnerability Assessment Program	FAA/TSA	1, 2

Annex B. Maritime

1 Executive Summary

Saltwater 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 that ply the maritime domain[137] are the primary mode of transportation for world trade, carrying more than 80 percent[138] of the world's trade by volume. U.S. maritime trade is integral to the global economy, representing more than 20 percent[139] of global maritime trade. Through the Maritime Transportation System (MTS),[140] the maritime mode is the primary transportation mode providing connectivity between the U.S. and global economies; 99 percent of overseas trade by volume enters or leaves the United States by ship.[141] The MTS enables the United States to project 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 are fundamentally linked to the health and functionality of the MTS.[142]

The security of the MTS is paramount to protecting the Nation and its economy; however, it presents daunting and unique challenges to managers of the maritime mode. The security of the MTS is intrinsically linked to the security of the maritime domain, which contains critical infrastructure and key resources (CI/KR) from many of the other critical infrastructure sectors and Transportation Systems Sector modes. Providing for the security of the MTS depends on an understanding of the diverse array of activities in the maritime domain through the transparency of all sector and transportation modal infrastructure and security activities.

The October 2005 National Maritime Transportation System Security Recommendations for the National Strategy for Maritime Security describe the Maritime Transportation System Security as:

> *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.*

[137] 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.
[138] Organization for Economic Co-operation and Development, *Security in Maritime Transport: Risk Factors and Economic Impact*, Maritime Transport Committee, July 2003, p. 6.
[139] National Chamber Foundation of the U.S. Chamber of Commerce, *Trade and Transportation, A Study of North American Port and Intermodal Systems*, Washington, DC, March 2003, p. 1.
[140] Also referred to as the Marine Transportation System. In the context of the Transportation Systems Sector, the U.S. Coast Guard is the Sector-Specific Agency for the maritime transportation mode, which may be also referred to as the maritime transportation systems mode.
[141] Committee on the Maritime Transportation System, *What is the MTS?*, www.cmts.gov//whatismts.htm.
[142] 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.

The maritime transportation security 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 CI/KR assets and resources of the system and its interconnecting links with other modes of transportation and CI/KR sectors:

- Maritime modal stakeholders are formalizing new coordination processes using the Sector Partnership Model espoused in the National Infrastructure Protection Plan (NIPP). The Maritime Modal Government Coordinating Council (GCC) has formed and the Maritime Modal Sector Coordinating Council (SCC) is in development.
- Maritime Domain Awareness (MDA), which allows for the effective understanding of anything associated with the global maritime domain that could impact the security, safety, economy, or environment of the United States, will be promoted. MDA is a foundational element of maritime security and CI/KR protection. It will enhance information sharing among Federal, State, local, and tribal authorities; the private sector; and international partners. This enriched information will be used by decisionmakers in determining response and risk management calculations for protecting maritime CI/KR and, in turn, the overall MTS.
- The Maritime Security Risk Assessment Model (MSRAM) assesses and manages risk for maritime infrastructure. A systems approach to risk management is being developed to improve efficiencies of resources and increase modal security.

2 Overview of Mode

The maritime transportation mode is unique in both its management and composition. The unique qualities of the mode present extraordinary complexity and challenges for those charged with the security of maritime critical infrastructure and key resources (CI/KR) and systems.

No single government agency possesses the responsibility for, the resources required, or the awareness needed for ensuring security in the maritime mode. The security of the mode depends on the cooperative actions of multiple Federal, State, local, tribal, and private entities, in addition to international partners. Prior to the National Infrastructure Protection Plan (NIPP), many varied processes provided the means for interagency coordination, including Policy Coordinating Committees, work groups, liaison officers, and Memorandums of Understanding (MOUs). While these means for coordination will continue, new constructs are being formed in accordance with the NIPP Partnership Model in an effort to better enable coordinated security across transportation modes.

The U.S. Coast Guard (USCG), as the Sector-Specific Agency (SSA) for the maritime transportation mode will continue to work collaboratively with the Transportation Security Administration (TSA); Customs and Border Protection (CBP); and other Federal, State, local, and tribal entities as the chair of the Maritime Modal Government Coordinating Council (GCC). The Maritime Modal GCC will work with industry security partners[143] to implement the NIPP requirements for CI/KR protection and help prevent, prepare for, protect against, respond to, and recover from transportation security incidents (TSIs), natural disasters, and other emergencies.[144] Other security partnerships include international cooperation vis-à-vis participation in international organizations and other multi-lateral and bi-lateral forums and exchanges.

The Maritime Transportation System (MTS) is a complex system that is geographically and physically diverse in character and operation. From a 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 chains or domestic commercial operations. The various maritime operations within the MTS networks have components that include vessels; port facilities; waterways and waterway infrastructure; and intermodal connections and users, including crew, passengers, and workers.

[143] See the NIPP, Glossary of Key Terms, June 2006
[144] The NIPP and the National Response Plan (NRP) together provide a comprehensive, integrated approach to the homeland security mission.

MTS components share critical interfaces with each other, with 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 CI/KR 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 sector and transportation modal infrastructure and security activities. The MTS and component CI/KR function as intermodal gateways for cargo flow to and from other CI/KR sectors. Significant economic and functional dependence exists within the transportation system on the timely and free flow of maritime commerce to and from homeland destinations. Because of the complexity, these interdependencies require any maritime security planning to be coordinated and aligned with any connecting transportation mode or sector.

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 effects of cargo and conveyance, combined with close proximity to surrounding industrial areas and communities, magnify the potential consequences of even a single-facility or single-vessel TSI with potential effects well outside of 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 National Strategy for Maritime Security (NSMS) defines Maritime Domain Awareness (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." The product of MDA is knowledge used by decisionmakers to determine the appropriate responses to maritime threats or to conduct further analysis. MDA is broken down into four activities: collection, fusion, analysis, and dissemination. Data and information on people, cargo, vessels, and infrastructure associated with the maritime domain are collected. (Collection is from all sources: classified sources, regulatory data, industry data, law enforcement, military, open sources, etc.) The data 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 includes the concerted efforts of Federal, State, local, and tribal authorities in conjunction with commercial stakeholders, foreign governments, and other international partners. MDA is a foundational element for security and CI/KR protection as the associated activities and results encompass the maritime domain and the MTS. The knowledge provided through the MDA effort can be used by decisionmakers in their response decisions and risk management calculations.

Maritime security partners will continue to work cooperatively to improve the existing baseline of maritime security planning efforts. Improvements to maritime homeland security will continue to build on lessons learned from ongoing operations; incident management training and exercises; research and development; science and technology; an improved common operating picture through improved MDA; and enhanced, interoperable information-sharing mechanisms.

3 The Maritime Transportation Mode

As previously discussed, the MTS is a highly 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:[145]

- 25,000 miles of navigable waters;
- 238 locks at 192 locations;
- The Great Lakes;
- Saint Lawrence Seaway;
- More than 3,700 marine terminals; and
- 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; 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:[146]

- Waterborne cargo and associated activities contribute more than $742 billion annually to the U.S. gross domestic product (GDP), sustaining more than 13 million jobs.
- In 2004, approximately 6,400 commercial ships made approximately 60,000 U.S. port calls, carrying more than 6 million cargo containers to the United States.
- In 2003 alone, more than 1.2 billion short tons of international maritime cargo were transported through U.S. seaports.
- Ninety-nine percent of the volume of overseas trade (62 percent by value) enters or leaves the United States by ship.

3.1 Vision and Goals[147]

The vision and goals of the Maritime Transportation Mode are:

Vision Statement for the 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 against or involving the use of MTS.

Objectives:

- Security partners will continue to develop and implement flexible, layered, security measures, both routine and random, while increasing security awareness training and security information sharing; and

[145] Additional information is available at Committee on the Marine Transportation System, What is the MTS?, www.cmts.gov//whatismts.htm.
[146] Id.
[147] See Transportation Systems SSP Base Plan for Transportation Systems Sector goals.

- Security partners will conduct combined drills and exercises to test, practice, and evaluate the execution of prevention/protection operations and contingency plans and procedures.

Goal 2: Enhance the resiliency of the MTS.

Objective:

- Security partners will reduce the risk associated with key nodes, links, and flows within critical MTS areas to enhance overall MTS survivability and continue to develop flexible contingency plans that are exercised and updated to ensure the most expeditious response and recovery to all-hazards events.

Goal 3: Maximize cost-effectiveness for the limited resources of the MTS.[148]

Objectives:

- Security partners will strive to align resources to the highest priority MTS security risks and continue to develop and disseminate standards for risk analysis tools and methodologies; and
- Define physical, cyber, and human elements in relation to the protection of maritime CI/KR.

3.2 Unique Characteristics of the Maritime Mode

The MTS depends on networks of critical infrastructure—both physical networks, such as the marine transportation system, and cyber networks, such as interlinked computer operations systems. The ports, waterways, and shores of the maritime transportation mode are lined with military facilities, nuclear power plants, locks, oil refineries, levees, passenger terminals, fuel tanks, pipelines, chemical plants, tunnels, cargo terminals, and bridges.

Ports, in particular, have inherent security vulnerabilities. Ports 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 persons gaining entry to collect information and commit unlawful or hostile acts.

The CI/KR within the maritime sector 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. Some physical and cyber assets, as well as associated infrastructure, also function as defense critical infrastructure; their availability must be constantly ensured for national security operations worldwide. Just-in-time methods, utilized within industries, must be considered for their implications on risk and vulnerability. Beyond the immediate casualties, the consequences of an incident on one node of maritime critical infrastructure may include disruption of entire systems, cause congestion and limit capacity for product delivery, cause significant damage to the economy, or create an inability to project military force. Protecting 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.

3.2.1 Key Components

Seaports and Marine Terminals

There are approximately 70 deep-draft port areas along U.S. coasts, including approximately 40 that each handle 10 million or more tons 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 and passenger movements. Terminals handling bulk cargoes 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

[148] To the greatest extent possible under the law.

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 account for 85 percent of all containership calls in the United States, and the port complexes in six 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, and Seattle/Tacoma. Tanker calls are likewise concentrated regionally. They are most frequent 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 several contain federally maintained channels used regularly by both passenger and cargo vessels. Located on the waterfront are publicly and privately owned marine terminals that consist of piers and berths for vessel docking. Most are privately operated and are designed to handle particular types of commodities. The 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 usually connected to rail sidings, roads that accommodate trucks, and pipelines. The terminal itself may be the origin or destination point for the cargoes moved on the waterways, as is the case for coal shipped to the dock of a waterfront power plant or chemicals shipped from a waterfront chemical plant.

Navigation Infrastructure and Services

U.S. waterways consist of thousands of miles of main channels, connecting channels, and berths. More than 90 percent of U.S. maritime trade passes through the more than 300 deep-draft navigation projects that the U.S. Army Corp of Engineers (USACE) maintains nationwide. USACE's responsibilities for inland waterways are complemented by the Department of Commerce National Oceanic and Atmospheric Administration's (NOAA's) responsibilities for coastal management to chart, preserve, enhance, and monitor 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. USCG maintains nearly 50,000 aids to navigation that range from lighted buoys and beacons to radio navigation systems. Responsibility for waterway management, including coordinating and controlling vessel operations and scheduling on the waterways, also includes, in addition to Federal agencies, local pilot associations, private marine exchanges, port authorities, and individual vessel operators.

Intermodal Connections

Intermodal transportation refers to a system that connects the separate transportation modes, such as Aviation, Maritime, Mass Transit, Highways, and Railroads, and allows a passenger or cargo to complete a journey using more than one mode. In terms of cargo transportation, an intermodal shipment is generally considered to be 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.

Oceangoing Vessels

Major classes of oceangoing vessels are tankers, containerships, 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. About two-thirds of these calls are made by tankers, containerships, and dry bulk carriers.

Passenger Carriers

Many of the passenger vessels operating in U.S. Territorial waters are ferries. Many carry automobiles and trucks, as well as passengers. Although they are important parts of the public transportation systems in cities such as Seattle, WA; San Francisco, CA; and New York, NY, passenger ferries account for a small percentage of the Nation's total passenger trips on all public transportation modes, including subways and urban buses. Likewise, passenger ocean liners no longer have significant roles in long-distance passenger transportation; they have been replaced by jet airplanes. Cruise ships continue to serve the recreation and tourism industries and operate on a regular basis from U.S. ports. In 2005, more than 9 million North Americans went on a cruise. The cruise industry also supports the economy. In 2004, cruise lines and their passengers spent $14.7 billion on U.S. goods and services, and supported more than 315,000 American jobs.[149]

Inland River, Coastal, and Great Lakes Systems

While the deep oceans are the primary means of moving cargo internationally, U.S. inland river, coastal, and Great Lakes waterways are important means of moving oceangoing cargo internally and for providing outbound feeder traffic for overseas shipping:

- Inland River Systems

  By far the largest and busiest inland waterway system in the United States 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 United States.

- Coastal and Intracoastal Waterways

  The main coastwise shipping activity in the United States occurs along the gulf coast and, to a lesser extent, along the Atlantic coast. The Gulf Intracoastal Waterway (GIWW), maintained by USACE for 1,300 miles from Texas to Florida, 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 rank among the top 50 U.S. ports in terms of tonnage, including Duluth–Superior, Chicago, Detroit, and Cleveland. The terminals in these ports, as well as most others on the Great Lakes, primarily handle dry bulk cargoes, led by iron ore, grain, coal, sand, stone, and lumber. Icebreaking operations maintain maritime travel and trade routes, allowing for mobility of law enforcement, defense assets, and essential resources. Access to and transit within the Great Lakes system requires close international cooperation with Canada.

Defense Port and Facility Prioritization

The Department of Defense (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 (DPA), 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.

[149] International Council of Cruise Lines, Inside Cruising: A Guide for Travel Professionals, www.iccl.org/faq/cruising.cfm.

The National Port Readiness Network (NPRN) helps train port and DoD personnel in using relevant emergency procedures and coordinates deployments through ports. NPRN comprises nine Federal agencies (MARAD, U.S. Transportation Command (USTRANSCOM), USCG, TSA, U.S. Northern Command (USNORTHCOM), Surface Deployment and Distribution Command (SDDC), USACE, Maritime Security Committee (MSC), and U.S. Forces Command (USFORSCOM)), with missions that support the secure movement of military cargo during deployments or other national emergencies. This training and coordination is accomplished through the local NPRN Port Readiness Committees.

3.2.2 The Regulatory Environment

Security partners derive their responsibilities, both individually and collectively, from several main sources: international agreements, treaties and conventions, legislation, executive directives, and assigned mission(s). Security partners have worked collectively and collaboratively to meet these responsibilities and to create a layered security regime. This layered regime includes the International Maritime Organization's International Ship and Port Facility Security Code (ISPS Code), which was championed by the United States and other contracting governments, and has since been implemented and continues to be monitored by the United States and other member states around the globe. The Maritime Transportation Security Act of 2002 (MTSA, Public Law 107-295), developed contemporaneously with the ISPS Code, implements security requirements on the U.S. maritime industry.

Figure 3-1 depicts some of the multiple executive and legislative requirements for maritime security planning that required the collaborative efforts of all maritime stakeholders. It also depicts the relationships between these planning efforts.

Security partners recognize that while not of all these responsibilities and requirements are derived for the explicit purpose of protecting critical infrastructure, most support infrastructure protection and indirectly support the NIPP.

3.3 NIPP Partnership and Information-Sharing Processes

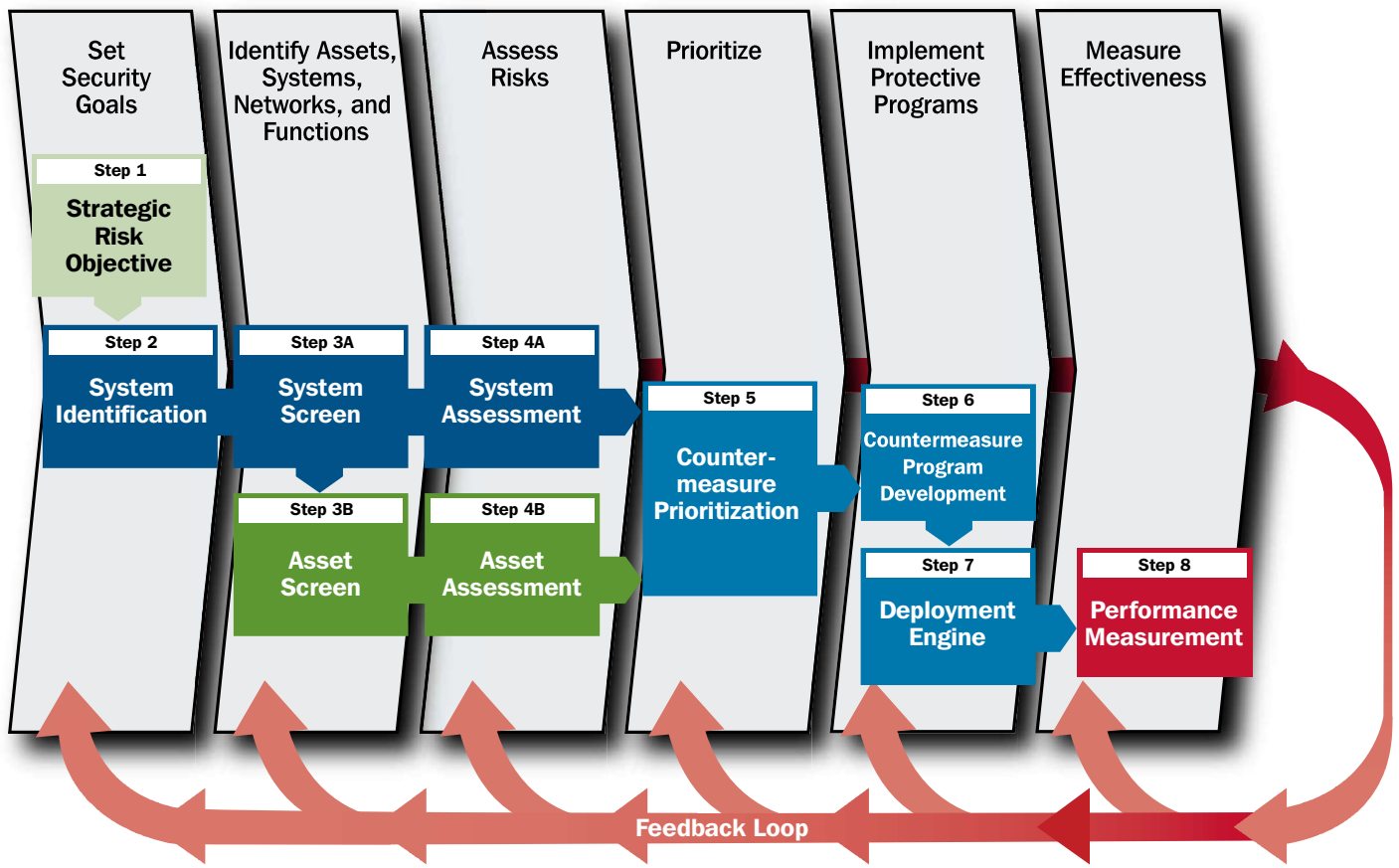
As described in the NIPP and the Transportation Systems Sector-Specific Plan (SSP) Base Plan, a network approach is used for information sharing among security partners in order to share and protect the information needed to analyze risk and make risk-based decisions to protect CI/KR. The NIPP defines the organizational structure that provides the framework for coordinating CI/KR protection efforts at all levels of government, as well as within and across sectors. Sector-specific planning and coordination are addressed through the private sector and GCCs that are established for each sector. Sector Coordinating Councils (SCCs) are comprised of private sector representatives of the SSAs; other Federal departments and agencies; and State, local, and tribal governments. These councils create a structure through which representatives from all levels of government and the private sector can collaborate or share existing consensus approaches to CI/KR.[150]

3.3.1 The Existing Process of Information Sharing

Information sharing between security partners is vital to the protection of CI/KR and the application of the NIPP risk management framework—from setting security goals to identifying assets, systems, networks, and functions; to assessing consequences, vulnerabilities, and threats; to prioritizing and implementing protective programs and their measures of effectiveness. Multiple information-sharing processes are in use by the government and the private sector. Information is often shared through public meetings such as Shipping Coordinating Committee meetings or other Federal Register notifications. Effective practices include information sharing vis-à-vis the Information Sharing and Analysis Center (ISAC), Homeport (described below), Area Maritime Security Committees (AMSCs), and through more recent initiatives such as the NIPP Partnership Model. The following information-sharing mechanisms are specific to the maritime transportation mode:

[150] See discussion in the NIPP, Organizing and Partnering for CI/KR Protection, p. 4.

Figure Annex B3-1: Example Maritime Security Planning Requirements



ISAC [151]

The Maritime ISAC is unique from other CI/KR ISACs in that it is not managed by the private sector. It is currently managed by the USCG Office of Port Activities and serves the purpose of facilitating 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.

The Maritime ISAC operates at the national, regional, and local levels and: (1) provides information on threats to the MTS, as well as information concerning incidents, threats, attacks, and vulnerabilities; (2) 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; (3) enables the maritime community to identify, report, and share information to reduce security vulnerabilities; and (4) 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 ISAC leverages the technology of Homeport, as an organized mechanism for the secure exchange, dissemination, coordination, and storage of sensitive information.

[151] 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, DC.

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 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[152]

Homeport is a publicly accessed and a 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).

Homeport meets the critical mission requirements in support of MTSA for information sharing and is used as a primary means for day-to-day management and communication of port security matters between public and private security partnerships 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.

Area Maritime Security Committees

USCG sponsors AMSCs to support all Captain of the Port zones. AMSCs fall under the jurisdiction of a USCG FMSC, who is also the USCG Captain of the Port for a particular port area or zone. AMSCs are a cornerstone of U.S. national maritime security by serving as formal bodies at the local (and sometimes regional) level for coordinating and collaborating among various Federal, State, and local authorities and private sector maritime stakeholders for enhancing and maintaining port security within a given area.

4 Implementation Plan

As discussed in other sections of this document, the security of the maritime domain and its inclusive infrastructure is not the province of any single security partner; it is the collective, collaborative effort of Federal, State, local, tribal, and private sector security partners. While security partners share and support the goals in section 3.1, each pursues these goals in accordance with its own requirements (i.e., business, mission, executive, or legislative). Government security partners execute their responsibilities either individually or as part of a larger collaborative effort by enforcing Federal regulations, programs, plans, and strategies. These cumulative activities implement the responsibilities of the security partners, which include, but are not limited to, the protection of CI/KR.

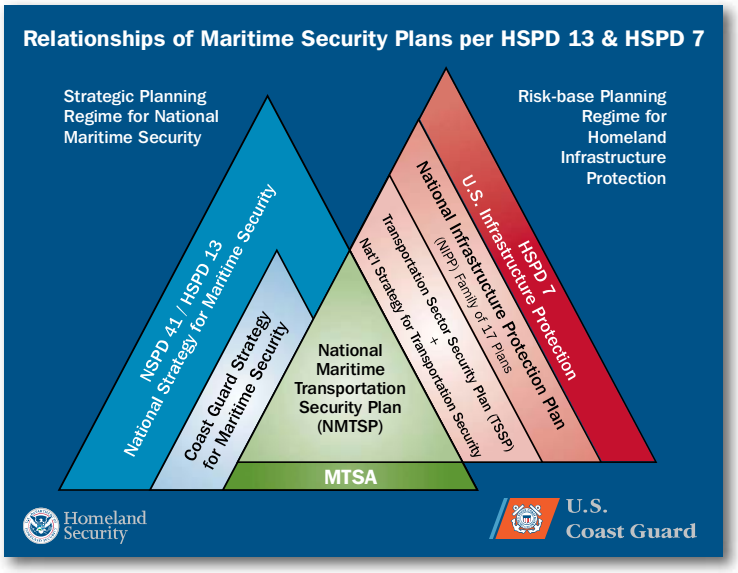
Figure 4-1 is a representative example of the concurrent implementation of three Federal security requirements. Note that while this example uses the USCG as the implementing agency, it is serving as a proxy for all Federal security partners.

The directives and plans establishing national maritime policy include :

- HSPD-7 establishes a national policy for Federal departments and agencies to identify and prioritize U.S. CI/KR and to protect them from terrorist attacks.
- National Security Presidential Directive 41 (NSPD-41)/HSPD-13 is a holistic approach to maritime security missions comprised of the NSMS and eight supporting plans to ensure the safety and economic security of the United States.
- The National Maritime Transportation Security Plan (NMTSP) implements 10 statutory requirements of MTSA and creates a three-tier maritime security planning regime.

[152] Additional information on Homeport is available at http://homeport.uscg.mil.

Figure Annex B4-1: Relationships of Maritime Security Plans per HSPD-13 and HSPD-7



Source: U.S. Coast Guard

The NMTSP is the capstone of the three-tier MTSA security planning regime, which includes Area Maritime Security Plans (AMSPs) and vessel and facility security plans. USCG provides guidance for the content of these plans and is responsible for inspecting and approving vessel and facility plans. AMSPs are developed with the assistance of AMSCs (comprised of Federal, State, local, and private security partners) and include a security assessment of the respective area. AMSPs are also informed by the NMTSP, which contains a National-Level Maritime Risk Assessment identifying the top 29 maritime threat scenarios and 53 recommended risk-reduction measures.[153] NMTSP is aligned with NSMS and has direct linkage by incorporating the NSPD-41/HSPD-13 Maritime Transportation System Security Recommendations by reference.

In addition, the NMTSP Plan to Re-Establish Cargo Flow After a Security Incident is aligned with the NSPD-41/HSPD-13 Maritime Infrastructure Recovery Plan (MIRP) to protect the economy of the United States by ensuring the continuity of maritime commerce and the MTS following a TSI. Both of these plans protect a critical infrastructure system using risk-based decisionmaking in close cooperation with State, local, tribal, and private security partners.

This example portrays how, within the maritime mode, a Federal agency must implement the requirements of the NIPP by implementing existing maritime security requirements. While the requirements address different aspects of maritime security, they are mutually linked and reinforce each other.

The planning and execution of these requirements with finite resources require alignment with the basic tenets of the NIPP, using Systems-Based Risk Management (SBRM) and including Federal, State, local, tribal, and private security partners to the maximum extent possible.

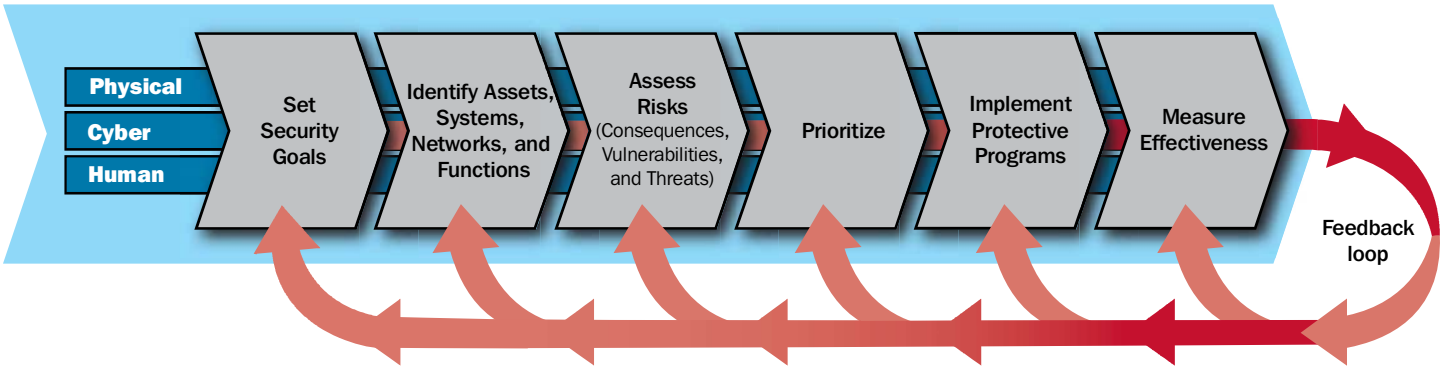
4.1 Approach for Achieving Sector and Modal Goals

By applying the NIPP risk management framework (see figure 4-2), security partners within the maritime transportation mode will continue to establish the processes for combining consequences, vulnerabilities, and threat information to produce a com-

[153] National Maritime Transportation Security Plan, Section III, December 2005. The NMTSP National Maritime Risk Assessment was conducted by a multi-agency work group; the risk reduction recommendations apply to all maritime security partners.

prehensive systematic and rational assessment of the MTS, thereby also contributing to the overall risk management framework for the Nation. Further details are described in section 3.

Figure Annex B4-2: NIPP Risk Management Framework



4.1.1 Assessing Risk and Prioritizing Assets and Systems

The primary tool used to assess risk to national infrastructure in the maritime domain is the Maritime Security Risk Assessment Model (MSRAM). MSRAM is a Risk Analysis and Management for Critical Assets Protection (RAMCAP)-compliant risk analysis tool used by USCG and other maritime industry stakeholders 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 CI/KR 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 = Threat x Vulnerability x Consequence and also considers area-wide security measures and response capabilities. As our understanding of system-wide risks mature, MSRAM, as with other risk measurement tools, will evolve to incorporate broader system assessment data.

4.2 Programs and Initiatives

The chart below shows a representative breadth of program initiatives[154] managed by agencies throughout the maritime mode. These programs may also support other mission areas within their multi-mission agencies and respective departments. The Maritime Mode has three goals each related to protecting the Maritime Transportation System. The Maritime Mode's goals are:

- Goal 1: Prevent and deter acts of terrorism involving use of or against the MTS.
- Goal 2: Enhance the resiliency of the MTS.
- Goal 3: Maximize cost-effectiveness for the limited resources of the MTS.

Department/Organization/Agency	MTS Program/Initiative	MTS Goal Supported
DHS/Multiple	National Strategy for Maritime Security	1, 2, 3
DHS/Multiple	National Infrastructure Protection Plan	1, 2, 3

[154] A recent DHS survey identified more than 260 national, department, and component security strategies, plans, programs, and regulatory requirements.

Department/Organization/Agency	MTS Program/Initiative	MTS Goal Supported
DHS/USCG	Operation Neptune Shield	1, 2, 3
DHS/USCG	Maritime Security Risk Assessment Management Tool	1, 2, 3
DHS/Multiple/Private Sector	Maritime Security Plans	1, 2, 3
DHS/USCG	Maritime Sentinel	1, 3
DHS/USCG/Private Sector	Information Sharing and Analysis Center	1
DHS/USCG/Private Sector	Homeport	1, 2
DHS/Multiple/Private Sector	Maritime Security Advisory Committees	1, 2, 3
DHS/CBP	24-Hour Advanced Cargo Manifest	1, 2
DHS/CBP	Container Security Initiative	1, 3
DHS/DOT/FAA/CBP	Advanced Passenger Information System	1, 3
DHS/CBP	Customs-Trade Partnership Against Terrorism	1, 3
DHS/DoD/DOS	Proliferation Security Initiative	1
DHS/USCG/CBP	Security Assessments	1
DHS/TSA/USCG	PortStep	1
DHS/TSA/USCG	Transportation Worker Identification Credential Program	1
DOJ/FBI	Maritime Liaison Agent Program	1, 2
DOJ/FBI	Joint Terrorism Task Forces	1
DOJ/FBI	InfraGard	1
DOJ/FBI	Field Intelligence Groups	1
DOT/MARAD	Maritime Security Professional Training	1
DOT/DHS/DoD	Port Readiness Committees	1, 2
DHS/USCG	Advanced Notice of Arrival (96 hours)	1
DHS/USCG	CoastWatch	1, 2
DHS/USCG	Maritime Intelligence Fusion Center	1, 2

Department/Organization/Agency	MTS Program/Initiative	MTS Goal Supported
DHS/USCG	USCG Field Intelligence Support Team	1, 2
DHS/DoD/DOJ	Maritime Operational Threat Response	1, 3
DOT/MARAD	SafePort	1, 2

4.3 Operations Scenario

From a system-of-systems perspective, MTS is a network of maritime operations that interface with shoreside operations at intermodal connections as part of overall 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, 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. Through security partnerships, the principles of *detect*, *deter*, and *defend* are employed to inevitably defeat the growing threat of global terrorism.

The following *scenario* portrays the operational process of protection by defense systems of what could occur on a given day, in a given port:

> A pilot boat drifts in 12-foot seas near the harbor entrance to a U.S. port waiting for an inbound container ship. On board that boat, in addition to the pilots, are members of the USCG's Vessel Boarding and Security Team (VBST) and agents of the U.S. CBP preparing to board the ship offshore. Their mission is to ensure that the ship doesn't diverge from its intended course as it enters the port and to verify the identity of the crew on board. Intelligence from international sources and the vessel's last ports of call expressed security concerns, subjecting the vessel to greater scrutiny and enhanced security measures.
>
> At the same time, the USCG's Vessel Traffic System (VTS) office monitors radar screens and computer displays. The VTS personnel analyze and assess data from Automated Identification System (AIS) signatures, radar contacts, and advanced Notice of Arrival (NOA) in an effort to maintain Maritime Domain Awareness (MDA) and to verify that all vessels in or approaching the port are cleared. An 87-foot USCG patrol boat from the local USCG sector stands ready to get underway to respond to unidentified contacts or suspicious vessels.
>
> Closer to port, the crews aboard two 25-foot armed small boats wait to escort the container ship to its berthing. These highly trained crews from the USCG's Maritime Safety and Security Teams (MSSTs) are well versed in tactics and procedures to ensure that no vessel approaches or threatens the inbound container ship.
>
> While these boats wait to begin the escort, members of the local USCGSector's Port State Control Teams arrive at the facility where the ship will moor. These inspection teams go aboard the ship and verify compliance with both the International Ship and Port Facility Code and Federal maritime security regulations.
>
> During the container ship's transit through the harbor, a passenger ferry passes by. Aboard the ferry are police officers from the local port authority and MSST explosives detection canine handlers. The two agencies randomly ride the ferries to screen passengers and belongings to prevent the introduction of explosives or weapons of mass destruction (WMDs) into the MTS.
>
> This scenario depicts the furtherance of the U.S. National Maritime Anti-Terrorism Strategy of detect, deter, defend, and defeat. Each aspect of the strategy is a coordination of international, national, State, and local resources and private maritime industry partners to effect a layered defense. The layered defense begins in international ports and continues to the high seas, the littorals, and finally into the ports and harbors of the United States.

Detect. Detection of potential threats to the United States is the most difficult phase of the national strategy. Detection begins with the U.S. security information community overseas. The U.S. CBP's Container Security Initiative (CSI), the Department of Energy's (DOE's) Megaports program, and the Department of State's (DOS's) Proliferation Security Initiative strive to detect dangerous cargos, illegal immigrants, and WMDs before they leave ports where vessels engaged in international voyages are served.

The National Vessel Maritime Intelligence Center under the CoastWatch program vets ship's crew and vessel port calls from submitted Notices of Arrival, and the CBP National Targeting Center conducts a risk-based analysis of vessel manifests for cargo, passengers, and crew. Additionally, CBP has the capability of arranging for the inspection of cargo overseas at 50 CSI ports, which cover 82 percent of maritime containerized import shipments. Locally, the FBI's Joint Terrorism Task Forces (JTTFs) and Field Intelligence Groups (FIGs), along with USGC's Field Intelligence Support Teams (FISTs), collect and analyze information from field-level personnel. This information comes from national, State, and local law enforcement; port operators; vessel operators; and local citizens to identify suspicious activities occurring in and around ports, terminals, waterways, and critical infrastructure in order to disrupt the planning of a potential terrorist attack.

Deter. The object of deterrence is to make a port, ship, or the Nation itself a difficult target for terrorists. USCG has led efforts for the United States in promoting deterrence among international trading partners, as with the creation of the International Port Security Program. International Port Security Liaison Officers (IPSLOs) are assigned to several locations worldwide to promote facility and vessel best practices.

U.S. law and regulations require port facility and vessel operators to conduct vulnerability assessments, create security plans, and implement security measures at their facilities and on their vessels to deter potential attackers. USCG enforces regulations that impose maritime security regulations. Facility and vessel inspectors ensure that training is conducted, security measures are in place and operational, and policies and procedures are being followed. A proactive deterrence method that is also being employed is randomization. Conducting random harbor patrols, recreational and commercial vessel boardings, facility patrols, helicopter overflights, passenger and cargo screening, and increased security measures are all conducted in coordination with local law enforcement to prevent predictability and deny potential attackers the ability to complete the planning phase of a terrorist attack.

Defend. Defending our Nation against its enemies is the first and fundamental commitment of the Federal Government. If detection and deterrence have failed, a well-planned strategic and tactical defense is required. Attacks of terrorism brought into focus the need to reexamine the requirements of domestic defense. The reexamination of defense was conducted with security partners, domestically and internationally. At the national level, several changes were made in the organization of the Federal Government. In the realm of maritime security, the most significant change brought together law enforcement and consequence management agencies to create the DHS, where USCG, TSA, and CBP, among others, now reside.

Within U.S. ports, commercial facility owners and operators are responsible for the safety and security of their own facilities during times of low threat. During periods of heightened threat, Federal, State, and local resources may be used to augment and, at times, assume responsibility for port security. To meet this need, USCG created 13 MSSTs that are located in strategic ports throughout the United States. These teams consist of highly trained law enforcement boarding personnel. They have been trained to use and have access to armed patrol boats, lethal and non-lethal defensive tactics, SCUBA equipment, underwater remote-operated vehicles, radiation detection equipment, and explosive detection canines. They work in conjunction with local police Special Weapons and Tactics (SWAT) teams, FBI Critical Incident Response Group tactical assets, and Navy Special Operations Forces to quickly thwart attacks and apprehend attackers.

Defeat. Defeating terrorism is a global endeavor. The DHS, DOS, DoD, the Department of Justice (DOJ), the Department of Transportation (DOT), and other agencies work closely with other countries to develop awareness, enhance collaborative security, and provide technical assistance to increase the capabilities of partner nation maritime services for mutual benefit.

Enhancing resiliency in the MTS, to quickly recover from the effects of a TSI, will minimize the ripple effects, protect the U.S. economy, and expedite the return to normalcy.

4.4 Metrics Process

The maritime transportation mode's sector-specific program measurement scheme will leverage existing information-sharing mechanisms and partnerships to measure progress toward Transportation Systems Sector goals. In general, measurement will begin with a periodic, scenario-based assessment of risk on the MTS, followed by estimations of the percentage of risk reduction credited to modal implementation plans. To evaluate across the breadth of goals, it will be desirable to estimate separately, the percentage of reductions to risk that occurs as a result of threat and vulnerability management (to track progress toward goal 1) and consequence management (for goal 2). Progress toward goal 3 will be informed largely by existing Office of Management and Budget (OMB)-inspired program efficiency measures. The existing AMSC structure and MSRAM will provide the correct starting venues for conducting this measurement analysis.

4.5 Effective Practices

The MTS is a regulated environment; government and industry build efficiency into the system through the use of effective practices. Industry best practices are pending formation of the SCC.

The following section describes some of effective practices in the MTS.

4.5.1 Security Guidelines

Security guidelines are recommended activities, implemented on a voluntary basis, that enhance the security of the MTS.

- **The Container Security Initiative (CSI).** CSI is a series of bilateral, reciprocal agreements that, among other things, positions CBP personnel at selected foreign ports to pre-screen U.S.-bound containers.
- **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 willing members of the trade community collaborate to better secure the international supply chain to the United States in support of homeland security. C-TPAT is one of CBP's initiatives that helps the agency achieve its twin goals: security and facilitation of trade moving into the United States.
- **America's Waterway Watch (AWW).** AWW is an outreach program, initiated by USCG, to enhance 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. USCG Reserve personnel concentrate on connecting with businesses and government agencies, while auxiliarists focus on building AWW awareness among the recreational boating public.

4.5.2 Security Requirements

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 are:

- Develop a three-tier maritime security regime:
  - 9,200 Domestic Vessel Security Plans; 3,200 Facility Security Plans;

  - 43 AMSPs; and
  - 1 NMTSP.
- Establish Security Advisory Committees:
  - National Maritime Security Advisory Committee (NMSAC); and
  - 47 AMSCs.
- Establish Maritime Security (MARSEC) levels set to reflect the prevailing threat environment to the maritime elements of the national transportation system. Maritime Security Directives are instructions issued by the Commandant, USCG, or designee, mandating specific security measures for vessels and facilities. MARSEC level descriptions and representative security activities are provided below:
  - **MARSEC 1:** MARSEC Level 1 is the level for which minimum appropriate protective security measures shall be maintained at all times. Focus on: Intelligence and Fusion, Harbor Patrols, Vessel Escorts, and Protection of Assets and Partnerships.
  - **MARSEC 2:** MARSEC Level 2 is 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. Increased: Air Surveillance, Critical Infrastructure Protection, Security Zone Enforcement, Cutters and Airborne Use of Force Deployed to Districts, Heightened Port Control, and Heightened Industry Security.
  - **MARSEC 3:** MARSEC Level 3 is the level for which specific protective security measures shall be maintained for a limited period of time when a TSI is probable or imminent, although it may be impossible to identify the specific target. Increased: Critical Infrastructure Protection, Maximum Port Control, Maximum Industry Security, Federal On-Scene Coordinator, Incident Command System (ICS), and WMD/Hazardous Materials Remediation.

Customs regulations require the advance and accurate presentation of cargo declaration information before loading cargo on a vessel at the foreign port (24-hour rule). Specifically, Customs Regulation 19 CFR 4.7 was amended to provide that, pursuant to 19 United States Code (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.

Vessels destined for a U.S. port or place must provide an NOA at least 96 hours in advance. The NOA requirements are found in 33 CFR 60.

Signed in October 2006, 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 that will 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 act establishes interagency operational centers for port security coordination and timetables and procedures for expediting the nationwide launch of the Transportation Worker Identification Credential (TWIC) program. It codifies a number of existing DHS cargo security programs, such as the CSI and C-TPAT programs. The act offers a plan to examine containers entering the United States for radiation and WMDs and provides for improvements in the Automated Targeting System. The SAFE Port Act also adopts the administration's establishment of the Domestic Nuclear Detection Office (DNDO). DNDO has extensive knowledge and involvement with the deployment of radiation portal monitors at ports of entry and other locations, and has been working closely with the National Institute of Standards and Technology (NIST) to determine the performance capabilities and validity of these instruments. The implementation of this act is in progress and will be discussed in greater depth in future versions.

4.5.3 Assessment and Compliance Process

Government agencies assess compliance with maritime regulations through two main processes:

- **Review and approval of regulatory requirements** backed by on-site inspections and spot checks. USCG publishes minimum required contents for MTSA-required vessel and facility security plans. These plans are reviewed and approved by USCG; compliance with these requirements is assessed during on-site inspections.
- **Compliance assessment** is the concept of layered defense. No single security program is a stand-alone program; however, each is part of a layered security regime. The scenario presented earlier highlighted the effects of this layering as multiple programs continuously assess cargo and persons being transported on the MTS. Cargo being shipped to the United States must be reported to CBP 24 hours prior to lading. A C TPAT partner's cargo shipping from a CSI port will still be reanalyzed by the National Targeting Center and the conveyance will make an NOA 96 hours before arriving at a U.S. port. Upon arrival, the conveyance is subject to boarding inspections and the cargo/personnel will need to clear customs before entering the United States through an intermodal gateway.

4.5.4 Training and Exercises Government Effective Practices

Training is an integral part of implementing protective programs and is conducted regularly by security partners. Exercises provide an opportunity to identify gaps in existing implementation plans while improving familiarity with the contents and competence in execution. While there are some regulatory requirements for training and exercises, other non-required training and exercise venues offer opportunities for collaboration among security partners. Scenario-based training can offer a systems perspective in the protection of critical infrastructure; participation in training and exercises occurs from the national to the local levels. Because no overarching training and exercise plan exists for the Nation, agencies will continue to meet training and exercise requirements for their individual agencies and seek to identify opportunities to incorporate modal security partners. The Sector Partnership Model provides forums to identify future opportunities to conduct both training and exercises, and to gain efficiencies and enhance knowledge management.

4.6 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 Goal and the associated National Priorities. Through its focus on port-wide risk management planning and domain awareness in the port environment, PSGP directly addresses six of the seven National Priorities:

1. Expanding regional collaboration;
2. Implementing the National Incident Management System (NIMS) and the National Response Plan (NRP);
3. Implementing the NIPP;
4. Strengthening information-sharing and collaboration capabilities;
5. Enhancing interoperable communications capabilities; and
6. Strengthening chemical, biological, radiological, nuclear, or (high-yield) explosive (CBRNE) detection and response capabilities.

In addition, PSGP also supports strengthening emergency operations planning and citizen protection capabilities, and assists in addressing security priorities specific to the port environment. PSGP uses a port-wide risk management program as part of urban area and State efforts. The process is patterned after the risk management framework articulated in the NIPP. Adopting a deliberate risk management planning process enables the FMSC and AMSC to make security enhancement decisions in the context of strategic security goals, supported by clear, measurable objectives. This process allows port area security needs to be integrated into the broader national risk management framework of the NIPP, into the regional planning construct that forms the core of the Urban Area Security Initiative (UASI) program, and into statewide initiatives. Similar to MTSA, the SAFE Port Act of 2006 requires that each grant be used to supplement and support, in a consistent and coordinated manner, the applicable Area Maritime Transportation Security Plan. Each grant is also coordinated with any applicable State or urban area homeland

security plan. The act also states that PSGP must take into account national economic, energy, and strategic defense concerns based on the most current risk assessments available.

4.7 The Way Forward

This modal implementation plan is the result of a collaborative effort between security partners in both the public and private sectors of the MTS. This plan captures how the maritime transportation mode, as a component of the Transportation Systems Sector, fits within the goals of the Transportation Systems Sector and how it contributes to the outcome of achieving these goals.

The MTS continues to evolve and respond to changes. The resultant cooperation and collaboration between and among existing and newly identified security partners continues to increase. From a systems perspective, communication is critical to the successful implementation of this plan, as well as the related family of plans. As NIPP partnerships evolve within the Transportation Systems Sector and the maritime transportation mode, so will a more mature risk-based methodology approach that will assist in the future identification and prioritization of resources for CI/KR protection.

The Departments of Homeland Security, Justice, Transportation, Commerce, Interior, and Defense all have a stake in MTS security. While USCG is designated as the lead DHS agency for maritime homeland security and the SSA for the maritime transportation mode, securing the MTS requires a team effort at all levels. The SSA is positioned to enable, assist, and collaborate with security partners in implementing, executing, and sustaining the processes and procedures necessary to secure the MTS in support of HSPD-7, HSPD-13, the NIPP, and other related plans.

The MDA Implementation Team, an interagency body of senior executives, is producing a Concept of Operations and an Investment Strategy that provides a structure under which maritime stakeholders within the Federal Government will align efforts to enhance MDA. The associated processes will be characterized by spiral development; as the relationships and partnerships in the MTS evolve, so will the information-sharing processes for MDA. MDA will evolve to include commercial, private sector, and international partners. These adaptable processes will adjust to the changing nature of the threats and associated risks, as well as to enhancements in supporting technologies.

Protecting and ensuring the continuity of U.S. maritime CI/KR is essential to the Nation's security, public health and safety, maritime commerce vitality, and the maritime sector way of life. Terrorist attacks on maritime CI/KR and other manmade or natural disasters could significantly disrupt the functioning of government and private sector businesses alike, and produce cascading effects far beyond the affected ports, waterways, and coastal areas of the actual incident location. Terrorist attacks using components of the MTS CI/KR as WMDs or disruption could have even more devastating physical, psychological, and economic consequences.

5 Program Management

Although the MTS and efforts to protect the CI/KR of the United States within the maritime domain are mature, the coordinating mechanisms stemming from the requirements of the NIPP are more recent. The maritime transportation mode will continue to evolve to meet these new requirements.

5.1 Coordinating Mechanisms

The SSA for the maritime transportation mode will continue to perform a leadership role alongside other SSA's as identified in the NIPP, continue to serve on the Transportation Systems Sector GCC, and continue to chair the Maritime Modal GCC. The SSA will use the Maritime Modal GCC to promote cooperative efforts among security partners to ensure that the modal implementation plan is updated using sanctioned communications processes and the Sector Partnership Model wherever possible.

In March 2006, the Maritime Modal GCC stood up as a subsector of the Transportation Systems Sector GCC. Primary membership as of November 2006 consists of representatives from:

- Department of Homeland Security:
  - Transportation Security Administration;
  - Customs and Border Protection;
  - DHS Office of Policy; and
  - DHS Office of Infrastructure Protection.
- Department of Transportation:
  - DOT Office of Policy; and
  - Maritime Administration.
- Department of Defense:
  - DoD Office of Transportation Policy; and
  - U.S. Army Corps of Engineers.
- Department of Commerce:
  - Transport and Security, Office of Service Industries.
- Department of Justice:
  - Federal Bureau of Investigation.

The responsibilities of the Maritime Modal GCC are derived from the NIPP and the charter of the Transportation Systems Sector GCC. Member agencies and representatives of the Maritime Modal GCC may also participate in other HSPD-7 designated CI/KR sectors and transportation modes.

The SSA and other Federal agencies within the maritime transportation mode have a long history of partnering with industry and the private sector to meet various safety and security goals. The Maritime Modal SCC will enable private sector security coordination and is currently under development.

5.2 Work Plan

The Maritime Modal GCC will form a work group to develop a 2- to 5-year work plan; the Sector Partnership Model will be used whenever possible. This work plan may consider:

- Identify forums and/or existing committees where synergy may be created by information sharing and collaboration with the Maritime Modal GCC;
- Examine and expand representation on Transportation Systems Sector GCC work groups, as applicable;
- Encourage maritime transportation mode representation on the Transportation Systems SCC;
- Expand MSRAM capabilities;
- Contribute to sector CI/KR Annual Report;
- Develop and define the future roles and responsibilities of the Maritime Modal GCC; and
- Identify methods and potential measures to be undertaken by government and/or the private sector to increase the efficiency of MTS infrastructure recovery and resumption of maritime trade following a significant incident.

Annex C. Mass Transit

1 Executive Summary

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

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

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

Critical systems and assets have been identified via a collaborative effort involving the Transportation Security Administration (TSA) and other components within the Department of Homeland Security (DHS), the Federal Transit Administration (FTA), the Federal Railroad Administration (FRA), the Federal Bureau of Investigation (FBI), mass transit and passenger rail agencies, and State and local governments. FTA, TSA, and other DHS components, in cooperation with State, local, and industry security partners, have conducted a number of vulnerability assessments of the systems and assets. Rail transit, commuter rail, and major transit systems have developed security plans and emergency preparedness plans in a format that is consistent with the FTA's Public Transportation System Security and Emergency Preparedness Planning Guide (2003). TSA's Surface Transportation Security Inspection Program (STSIP) continues these efforts with the Baseline Assessment and Security Enhancement (BASE) program. The BASE program reviews transit system implementation of 17 Security and Emergency Preparedness Action Items (Security Action Items (SAIs)), jointly developed by TSA and FTA in coordination with the Mass Transit SCC. Additionally, STSIP offers the Security Analysis and Action Program (SAAP), which constitutes a systematic vulnerability assessment of mass transit or passenger rail systems. The program utilizes several different tools to identify vulnerabilities based on specific scenarios, such as an improvised explosive device (IED) on a passenger train. SAAPs can be conducted on individual critical infrastructure facilities or entire rail systems, with particular emphasis on critical control points.

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

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

2 Mass Transit and Passenger Rail

2.1 Vision of Mode

Vision Statement for the Mass Transit and Passenger Rail Mode

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

Since the attacks of September 11, 2001, the more recent attacks on transportation targets such as the 2005 London bombings, and the coordinated attack on four commuter trains in Madrid in 2004, the mass transit and passenger rail industry has made

great strides in managing and mitigating risk and enhancing the security of the systems. Many of the systems have prepared security and emergency plans, developed and implemented enhanced awareness and training programs for employees and the public, expanded emergency drills and exercises, improved their surveillance and detection capabilities, hardened and improved access control for critical assets and systems, and deployed various security enhancement technologies. Some have engaged in limited screening activities and deployed law enforcement surge teams, initiated or enhanced explosives detection canine programs, and participated in testing and development programs for emerging security technologies. As a whole, the mass transit and passenger rail industry has been alert, diligent and innovative in enhancing the security of the employees and the traveling public.

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

The Transportation Security Administration (TSA) focuses particular attention on six transit security fundamentals that provide the foundation for a successful security program:

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

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

Enhancing transportation security requires a layered approach, integrating intelligence collection and analysis and law enforcement investigations to thwart plans before execution with the application of security resources and visible and random activities in ways that maximize the deterrent effect. The DHS, through its Office of Intelligence and Analysis, and the TSA, through its Office of Intelligence, integrate with the U.S. intelligence community to ensure continual situational awareness. These offices develop intelligence products and informational materials that inform the efforts of governmental decisionmakers and transit system operators and security officials. This concerted effort aims to track potential threats, disrupt their development, and focus Federal security resources and activities, as necessary, for detection, deterrence, and prevention.

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

Figure Annex C2-1: Operating Principles

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

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

2.2 Description of Mode

2.2.1 Overview

The Mass Transit and Passenger Rail Mode includes service by buses; rail transit (commuter rail; heavy rail, also known as subways or metros, and light rail, including trolleys and streetcars); long-distance rail, namely Amtrak® and Alaska Railroad; passenger ferryboats; and other, less common types of service (cable cars, inclined planes, funiculars. and automated guideway systems). It also includes on-demand 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, schoolbus systems, and private shuttle system operators.

Approximately 6,000 transit service providers; commuter railroads; and long-distance passenger railroad providers operate in the United States. The majority of these agencies operate more than one mode of service. Approximately 2,000 agencies provide bus service; 5,300 agencies operate on-demand services; and 150 agencies operate other forms of transportation, such as inclined planes or waterborne services.[155] There are 565 transit systems that operate in urbanized areas of a population greater than 50,000 persons. Additionally, Amtrak® operates the Nation's primary intercity passenger rail service over a 22,000-mile-long network, primarily over leased freight railroad tracks. As part of an intermodal system of transportation, the Mass Transit and Passenger Rail Mode is also connected to other modes of transportation through multi-modal systems and within multi-modal infrastructures.

In 2006, Americans took 9.7 billion trips using mass transit and passenger rail. Since 1995, ridership in the United States has grown by more than 23 percent; this is a faster rate than for highway travel. The American Public Transportation Association (APTA) estimates that about 33 million trips are taken each weekday in the United States. Heavy rail systems (subway systems such as the New York City transit system and the Washington, DC, Metro) typically operate in dedicated rights-of-way within a metropolitan area, draw electric power from a third rail, and have the capacity for a heavy volume of traffic. Commuter rail

[155] FTA National Transit Database, www.ntdprogram.com/ntdprogram.

systems, which often share operation on freight railroad tracks, consist of a diesel- or electric-powered locomotive and a set of passenger railcars and provide regional service (e.g., between a central city and the adjacent suburbs). Light rail systems are typically characterized by lighter weight passenger railcars, drawing electric power from overhead power lines, and often operate in shared-use rights-of-way, including streets with vehicular traffic.

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

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

Figure Annex C2-2: Significant Benefits of Mass Transit

Significant Benefits of Mass Transit	
• Easing Traffic Congestion	• Providing Access for Rural Areas
• Creating and Sustaining Jobs	• Improving Air Quality
• Providing Access to Jobs	• Reducing Energy Consumption
• Stimulating Economic Development	• Saving Money
• Boosting Real Estate Values	• Enhancing Mobility During Emergencies
• Fostering More Livable Communities	• Ensuring Safety
• Providing Mobility for Seniors	

2.2.2 Responsibilities

Securing the Nation's mass transit and passenger rail systems is a shared responsibility requiring coordinated action by Federal, State, and local governments; the public transportation agencies; their employees; and the passengers who ride these systems. Since the attacks on 9/11, the role of the Federal Government in this area continues to evolve. Prior to 9/11, DOT (namely, FTA and FRA) was the primary Federal entity involved in mass transit and passenger rail security matters. In response to the attacks on 9/11, Congress enacted the Aviation and Transportation Security Act (ATSA), which created TSA within DOT and defined its primary responsibility as ensuring security in all modes of transportation. The act also gave TSA regulatory authority and responsibility for security over all transportation modes. With the passage of the Homeland Security Act of 2002[156], TSA was transferred, along with more than 20 other agencies, to the DHS.

In executing its responsibilities and duties, TSA is specifically empowered to develop policies, strategies, and plans for dealing with threats to transportation.[157] 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.[158] TSA also is to enforce security-related regulations and requirements,[159] oversee the imple-

[156] Public Law 107-296.
[157] 49 United States Code (U.S.C.) 114(f)(3).
[158] Id., 114(f)(1)-(5).
[159] Id., 114(f)(7).

mentation and ensure the adequacy of security measures at transportation facilities,[160] and carry out other appropriate duties related to transportation security.[161] TSA has broad regulatory authority to achieve ATSA's objectives, and may issue, rescind, and revise such regulations as are necessary to carry out TSA functions, including issuing regulations and security directives without notice or comment or prior approval of the Secretary of Homeland Security if determined to be necessary to protect transportation security.[162] TSA is also charged with serving as the primary liaison for transportation security to the intelligence and law enforcement communities.[163]

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

TSA has implemented its authority for mass transit and rail security in a number of ways. In the aftermath of the attacks on commuter trains in Madrid in March 2004, TSA issued two security directives applicable to passenger rail and rail transit. The directives, designated SD RAILPAX-04-01 and SD RAILPAX-04-02, mandate specific measures intended to enhance the security of the U.S. Mass Transit and Passenger Rail Mode. The measures required by the directives support DHS's overarching goals to prevent, protect, respond, and restore. They have the force of regulations and remain valid and effective until revised or superseded by subsequent action by TSA.[164]

FTA conducts a range of non-regulatory safety and security activities, including safety- and security-related training, research, technical assistance, and demonstration projects. In addition, FTA promotes safety and security through its grantmaking authority. FTA provides financial assistance to public transportation agencies, through both formula-based and discretionary grants, to plan and develop new systems and operate, maintain, and improve existing systems. FTA stipulates the conditions of grants, such as certain safety and security statutory and regulatory requirements, and may withhold funds for non-compliance. FTA annually awards more than $3.5 billion in capital improvement grants. For formula-based grants, such as FTA's Section 5307 program, transit agencies are required to spend 1 percent or more of their annual allocations on security-related projects, or certify that they do not need to do so (based on criteria such as adequate non-Section 5307 funds being available for funding security needs or assessments indicating no deficiencies). For transit agencies in areas with more than 200,000 population, only security-related capital projects are eligible to meet the 1 percent threshold. Transit agencies in areas with less than 200,000 population can apply both capital and operating security expenses (such as the cost of security staffing) to meet the 1 percent threshold. Additionally, under the Safe, Affordable, Flexible, Efficient Transportation Equity Act: A Legacy for Users (SAFETEA-LU),[165] the definition of capital programs has been expanded to include security and emergency planning and training and exercises, thus providing more flexibility to larger transit agencies in meeting the 1 percent threshold.

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

State and local governments, mass transit and passenger rail operators, and private industry are also integral to the Nation's mass transit and passenger rail security efforts. State and local governments might own or operate a significant portion of the passenger rail system. Even when State and local governments are not owners and operators, they are directly affected by mass transit and passenger rail systems that operate within and through their jurisdictions. Consequently, the responsibility for responding to emergencies involving the mass transit and passenger rail infrastructure often falls to State and local governments. Mass transit and passenger rail operators, which can be public or private entities, are responsible for administering and

[160] Id., 114(f)(11).
[161] Id., 114(f)(15).
[162] Id., 114(l).
[163] Id., 114(f)(1) and (5).
[164] Id., 114(f)(1) and (5).
[165] Public Law 109-59, August 10, 2005.

managing related activities and services, including security. Passenger rail operators can directly provide the service or contract for all or part of the service. Although all levels of government are involved in mass transit and passenger rail security, the primary responsibility for implementing the security measures and activities rests with the operators.

2.2.3 Risk to Mass Transit System

Between 1995 and June 2005, there were more than 250 terrorist attacks worldwide against rail targets, resulting in nearly 900 deaths and more than 6,000 injuries.[166] These figures predate the London attacks of July 2005 and the Mumbai, India, attacks of July 2006 and do not include the persons killed and injured in those incidents.

Mass transit and passenger rail systems carry a large number of passengers every day and are open and fully accessible. For example, on average, more than 306,000 customers use the San Francisco Bay Area Rapid Transit (BART) system daily. Additionally, the Chicago Transit Authority's 1,190 rail rapid transit cars operate over more than 7 routes and 222 miles of track, providing 500,000 customer-trips each day, serving 144 stations. Unlike air transport, no access control or seat assignment is generally applied. The wide geographical coverage of mass transit and passenger rail networks provide numerous options for access and getaway. Multiple stops and interchanges lead to high passenger turnover, which is difficult to monitor effectively. The disruption of an entire operation can confuse the public and lead to panic, just as it can curtail mobility. The extensive and worldwide media coverage that potential attacks can generate not only affects the image of public transport, but also discredits Federal, State, and local governments. In line with the logic of its perpetrators, a potential terrorist attack on public transportation systems can result in a large number of victims, thereby achieving its desired effect. The recent examples of the Mumbai, London, and Madrid bombings—all involving use of multiple improvised explosive devices (IEDs)—are tragic reminders of this reality.

The consequences of an attack depend on the type of attack and the form of transportation. In a mass transit bus with a capacity of approximately 65 passengers, an attack would be significant. Subway and passenger rail trains present even greater potential consequences because of the higher number of passengers and cars and the enhanced effects of attacks in confined spaces that 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 these tunnels, as well as moving trains and ventilation shafts, can facilitate distribution of a chemical or biological agent throughout its facilities and, because of exterior vents and station egress points, can affect areas of a city. A terrorist can attack a subway system by releasing a chemical/biological weapon in a station, subway car, tunnel, or through a ventilation shaft. A transit bus explosion in a crowded highway tunnel could have dire consequences as well.

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

2.3 Transit, Commuter, and Long-Distance Rail GCC and SCC Structure and Process

The Transit, Commuter, and Long-Distance Rail Government Coordinating Council (TCLDR-GCC) was established in March 2006. Members of the TCLDR-GCC include TSA, DHS, DOT, the Department of Justice (DOJ), and, when appropriate, the Department of Defense (DoD). Appropriate State and local representation is also being coordinated. Outreach to stakehold-

[166] RAND Corporation, Memorial Institute for the Prevention of Terrorism (MIPT) Terrorism Knowledge Base, www.tkb.org/Home.jsp.

ers in the mass transit and passenger rail community encouraged establishment of a modal coordinating council for the Mass Transit and Passenger Rail Mode. With APTA acting as the Secretary to the Council, the Mass Transit Sector Coordinating Council (SCC) has been organized around an existing body of the APTA Security Affairs Steering Committee. Representing corporate and employee interests, participating entities include APTA, the Community Transportation Association of America, the Amalgamated Transit Union, Amtrak®, and individual transit agencies representative of the community in system size and geographic spread, as well as representation of business organizations providing support services to the public transportation industry. Additions may be made to this group to ensure a more robust and broad private sector engagement. Both the TCLDR-GCC and Mass Transit SCC commit to ensuring that the status of their respective members ensures their capability to affect decisions as may be required.

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

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

3 Implementation Plan

3.1 Goals, Objectives, and Programs/Processes

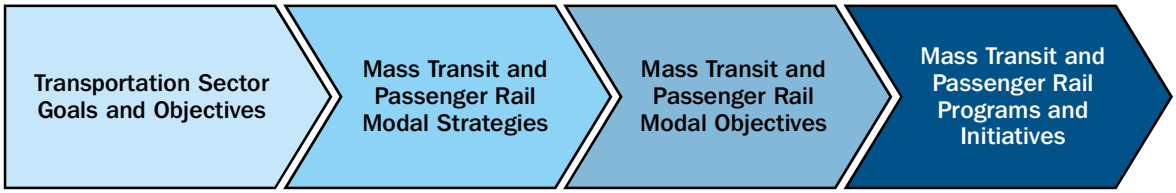
The Transportation Systems SSP identifies a set of goals and objectives for the Transportation Systems Sector. Achieving these goals and objectives requires a strategic approach that integrates the needs and requirements of the private sector through a meaningful collaboration between public and private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

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

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

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

Figure Annex C3-1: Process Model



The goals and objectives presented in the Transportation Systems SSP are:

- Preventing and deterring acts of terrorism using or against the U.S. transportation system;
- Enhancing the resiliency of the U.S. transportation system; and
- Improving the cost-effective use of resources for transportation security.

3.1.1 Expanding Partnerships for Security Enhancement

A close partnership with the appropriate parties is paramount to enhancing the security of mass transit and passenger rail, and is an integral element of the overall strategy. As discussed above, we are furthering this strategy through constructive engagement with: (1) governmental security partners via the TCLDR-GCC, (2) transit system operating and security officials via the Mass Transit SCC and Transit Policing and Security Peer Advisory Group, and (3) regional partners through the encouragement of regional coordinating councils.

Additionally, through regional engagement and regional deployment of resources, we are enabling the use of a full spectrum of available resources from Federal, State, and local governmental entities and the area transit systems that aims to disrupt the terrorists' ability to orient planning and preparation activities. This regional deployment approach entails developing and implementing a sustainable program to elevate security postures through visible and random deterrent activities and to enhance vigilance through security training and awareness programs. The Federal security teams coordinate with transit and passenger rail agencies in advance to effectively integrate with local targeted force packages to enhance security. These teams, consisting of Surface Transportation Security Inspection Program (STSIP) inspectors, Federal Air Marshals, explosives detection canine teams, and others, help expand application of visible, random, unpredictable security activities throughout the transit and passenger rail system, and set the foundation for sustained collaboration through existing surface transportation coordinating committees or regional GCC/SCC structure. Federal resources will be deployed in a manner that is consistent with the operational environment of transit services.

3.1.2 Continuously Advancing the Security Baseline

Establishing security guidelines and action items to help elevate the security baseline and posture is a major priority for mass transit and passenger rail security. TSA and FTA recently finalized a collaborative effort, coordinated with the Mass Transit SCC for review and input, to update the 20 security action items that FTA developed in the aftermath of 9/11. The new action items for transit agencies represent a comprehensive update addressing the new security threats and risks that confront transit agencies today, and priority areas with gaps in security and emergency preparedness programs. The security action items and the six transit security fundamentals support achievement of the goals and objectives articulated in the National Infrastructure Protection Plan (NIPP) and the Transportation Systems SSP, and the mandates of Executive Order 13416, Strengthening Surface Transportation Security. STSIP, through inspections, assessments, and technical assistance, together with the systems' self-assessments and other efforts by governmental and industry partners discussed throughout this plan, advance security baselines and enhance security postures throughout the Mass Transit and Passenger Rail Mode.

3.1.3 Building Security Force Multipliers

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

Since 9/11, mass transit and passenger rail agencies have developed and implemented public awareness materials that are both general and specific with their message. More recently, public awareness campaigns have been expanded to include a focus specifically on unattended bags and emergency evacuation procedures. The Federal Government has partnered with industry and labor representatives in several public awareness efforts, as explained in the programs/processes section of this annex. For example, TSA partners with FTA in Transit Watch, a program focused on developing and widely disseminating public awareness materials that mass transit and passenger rail agencies may adapt for their particular circumstances and use throughout their systems. Two particularly successful Transit Watch campaigns have been Is This Your Bag? and the See Something? Say Something! messages that remind mass transit riders to report suspicious bags or behavior, thereby empowering riders to become the eyes and ears of mass transit.

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

3.1.4 Providing Security Information to Leadership

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

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

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

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

Finally, the comprehensive information strategy meets six of the seven security priorities identified in HSPD-8, National Preparedness. The strategic objective of information dominance supports the National Incident Management System and execution of the National Response Plan. Close collaboration among governmental entities and with public transportation stakeholders through the GCC/SCC framework and CIPAC process implements the NIPP. Extending these forums by emphasizing the establishment of regional GCCs and SCCs expands regional collaboration across the mode and the Transportation Systems Sector. These collaborative efforts focus specifically on strengthening information sharing; interoperable communications; and detection, response, and disposal or decontamination of IEDs, including those with chemical, biological, radiological, or nuclear capability.

3.1.5 Deploying Tools to Mitigate High-Consequence Risks

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

Many transit systems across the United States are attempting to add increased technology to their layered security approach. Some examples include the investment of millions of dollars in surveillance and intrusion detection technology throughout their systems, satellite-based systems for bus tracking, and the testing of onboard cameras that can wirelessly transmit live color images.

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

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

3.1.6 Mass Transit Objectives

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

Figure Annex C3-2: 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 the bags of passengers entering the system.
• Effect a regional approach through coordinated planning among Federal regional officials (FSD, Federal Air Marshal Special Agent in Charge, STSIP, explosives detection canine teams, FBI); 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 the system.
• Conduct Security Readiness Assessments through collaborative efforts between area STSIP inspectors and transit security officials to conduct security assessments under the Security Analysis and Action Program and the Baseline Assessment and Security Enhancement (BASE) program.
• Coordinate with system security officials to examine the capabilities of transit agencies and frontline employees in identifying and reporting suspicious items and activities (entails setting unattended packages or staging other suspicious activities within the system to test awareness and reporting by employees and passengers).
• Improve Intelligence and Security Outreach through coordination between TSA's Office of Intelligence and the Transportation Sector Network Management (TSNM) Mass Transit Division, STSIP inspectors, and the regional intelligence and information-sharing centers to be implemented through regional engagement.
• Coordinate focused transit system employee training (TSA and FTA lead): (1) align program with the needs and requirements of mass transit or passenger rail security officials, and (2) sustain training emphasis through continuing regional engagement and coordination by field presence (regional directors of STSIP and FTA regional officials).
• Employ all available media/public address system announcements; billboards and posters; brochures; and reminding keepsakes, such as the keychain flashlights disseminated by TSA in DC's Washington Metropolitan Area Transit Authority (WMATA) system: (1) use varying messages and multiple media to engage and retain public interest, and (2) integrate TSA materials in a joint program.

3.2 Security Programs and Processes

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

Working Groups

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

Pursuant to this annex, the DHS and DOT agreed to coordinate their programs and services (including risk assessments, grants, training, exercises, and technical assistance) to better assist transit agencies in prioritizing and addressing their current and emerging security-related needs. The areas of coordination identified in the annex include training courses; awareness programs (i.e., Transit Watch); forums to encourage and facilitate communications and information sharing (i.e., the Safety and Security Roundtables); drills and exercises; emergency preparedness and security forums (i.e., the Connecting Communities forums on emergency preparedness and security); the creation of a comprehensive source for transit system officials to turn to for information about available Federal security and preparedness resources (e.g., information on grant funding availability, training, technical assistance, and effective practices); risk assessment and security reviews; and interoperable communications.

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

Figure Annex C3-3: Security Programs/Goals/Objectives

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

Programs	Goals	Objectives
Explosives Detection Canine Teams	**Goal 1:** Prevent and deter acts of terrorism using or against the transportation system.	**Objective A:** Implement risk-based flexible, layered, and unpredictable security programs. **Objective B:** Increase the vigilance of travelers and transportation workers (e.g., through security awareness information).
	Goal 2: Enhance the resiliency of the U.S. transportation system.	**Objective A:** Assess, manage, and reduce the risks associated with key nodes, links, and flows within critical transportation systems (e.g., robustness, redundancy, and technology).
	Goal 3: Improve the cost-effective use of resources for transportation security.	**Objective A:** Align sector resources with the highest priority transportation security risks using both risk and economic consequences as decision criteria. **Objective B:** Maximize sector participation as a partner in the development and implementation of public sector programs for critical infrastructure and key resources (CI/KR) protection.
Visible Intermodal Prevention and Response (VIPR) Teams	**Goal 1:** Prevent and deter acts of terrorism using or against the transportation system.	**Objective A:** Implement risk-based flexible, layered, and unpredictable security programs. **Objective B:** Increase the vigilance of travelers and transportation workers (e.g., through security awareness information). **Objective C:** Enhance information and intelligence sharing among Transportation Systems Sector security partners (e.g., Federal, State, local, and tribal governments; the private sector; and international security partners).
	Goal 2: Enhance the resiliency of the U.S. transportation system.	**Objective A:** Assess, manage, and reduce the risks associated with key nodes, links, and flows within critical transportation systems (e.g., robustness, redundancy, and technology).
Information Sharing • Mass Transit and Passenger Rail Information Sharing Network • National Resource Center	**Goal 1:** Prevent and deter acts of terrorism using or against the transportation system.	**Objective C:** Enhance information and intelligence sharing among Transportation Systems Sector security partners (e.g., Federal, State, local, and tribal governments; the private sector; and international security partners).

Programs	Goals	Objectives
Security Training and Awareness Programs • Connecting Communities • Safety and Security Roundtables • FLTEC Land Transportation Anti-Terrorism Training • Transit Watch • Interactive Computer-Based Training for Railroad Employees • Random High-Visibility Passenger Awareness	**Goal 1**: Prevent and deter acts of terrorism using or against the transportation system.	**Objective B:** Increase the vigilance of travelers and transportation workers (e.g., through security awareness information).
	Goal 2: Enhance the resiliency of the U.S. transportation system and perform collaborative risk analysis processes.	**Objective B:** Ensure the capacity for rapid response and recovery to all-hazards events (e.g., flexibility, timeliness, etc.).
	Goal 3: Improve the cost-effective use of resources for transportation security.	**Objective C:** Improve Transportation Systems Sector security research, development, test, and evaluation (RDT&E) resource allocation (e.g., leveraging technological expertise, minimizing redundancies).
National Tunnel Security Initiative	**Goal 1:** Prevent and deter acts of terrorism using or against the transportation system.	**Objective A:** Implement risk-based flexible, layered, and unpredictable security programs. **Objective C:** Enhance information and intelligence sharing among Transportation Systems Sector security partners (e.g., Federal, State, local, and tribal governments; the private sector; and international security partners).
	Goal 2: Enhance the resiliency of the U.S. transportation system.	**Objective A:** Assess, manage, and reduce the risks associated with key nodes, links, and flows within critical transportation systems (e.g., robustness, redundancy, and technology). **Objective C:** Develop, disseminate, and promote the adoption of a standard risk-reduction methodology.
	Goal 3: Improve the cost-effective use of resources for transportation security.	**Objective A:** Align sector resources with the highest priority transportation security risks using both risk and economic consequences as decision criteria. **Objective B:** Maximize sector participation as a partner in the development and implementation of public sector programs for CI/KR protection. **Objective C:** Improve Transportation Systems Sector security RDT&E resource allocation (e.g., leveraging technological expertise, minimizing redundancies). **Objective D:** Ensure that the public sector funds expended have achieved the expected risk reduction.

Programs	Goals	Objectives
Security Technology Deployment	**Goal 1:** Prevent and deter acts of terrorism using or against the transportation system.	**Objective A:** Implement risk-based flexible, layered, and unpredictable security programs. **Objective B:** Increase the vigilance of travelers and transportation workers (e.g., through security awareness information).
	Goal 2: Enhance the resiliency of the U.S. transportation system.	**Objective A:** Assess, manage, and reduce the risks associated with key nodes, links, and flows within critical transportation systems (e.g., robustness, redundancy, and technology).
	Goal 3: Improve the cost-effective use of resources for transportation security.	**Objective A:** Align sector resources with the highest priority transportation security risks using both risk and economic consequences as decision criteria. **Objective B:** Maximize sector participation as a partner in the development and implementation of public sector programs for CI/KR protection. **Objective C:** Improve Transportation Systems Sector security RDT&E resource allocation (e.g., leveraging technological expertise, minimizing redundancies).
Technology Research and Development	**Goal 1:** Prevent and deter acts of terrorism using or against the transportation system.	**Objective A:** Implement risk-based flexible, layered, and unpredictable security programs. **Objective B:** Increase the vigilance of travelers and transportation workers (e.g., through security awareness information).
	Goal 3: Improve the cost-effective use of resources for transportation security.	**Objective C:** Improve Transportation Systems Sector security RDT&E resource allocation (e.g., leveraging technological expertise, minimizing redundancies).
International Initiatives	**Goal 1:** Prevent and deter acts of terrorism using or against the transportation system.	**Objective C:** Enhance information and intelligence sharing among Transportation Systems Sector security partners (e.g., Federal, State, local, and tribal governments; the private sector; and international security partners).
	Goal 2: Enhance the resiliency of the U.S. transportation system.	**Objective B:** Ensure the capacity for rapid response and recovery to all-hazards events (e.g., flexibility, timeliness, etc.).

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

3.2.1 Surface Transportation Security Inspection Program (STSIP)

The DHS appropriations acts for 2005 and 2006 allocated funds for the hiring and deploying of "Federal rail compliance inspectors" (2005) and "rail inspectors" (2006). TSA created STSIP and deployed 100 rail inspectors to 19 field offices through-

out the United States, covering key rail and mass transit facilities throughout the regions. The program focuses on nationwide outreach and liaison activities with the rail industry and initiatives to enhance security in mass transit and passenger rail systems. These efforts include assessment programs specifically intended to expand TSA's domain awareness, elevate the security baseline throughout the mode, and assist systems in identifying and mitigating security vulnerabilities.

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

Additionally, TSA surface inspectors are actively engaged in performing Security Analysis and Action Program (SAAP) assessments, which constitute a systematic examination of stakeholders' operations to assess compliance with security requirements; identify security gaps; develop effective practices for sharing across the mode; and gathering baseline information on the system, its operations, and its security resources and initiatives. The program utilizes several different tools to identify vulnerabilities based on specific scenarios, such as an IED on a passenger train. SAAPs can be conducted on individual critical infrastructure facilities or entire rail systems, with a particular emphasis on critical control points. As a component of these evaluations, TSA focuses particular attention on six transit security fundamentals, explained in section 3.4, that provide the essential foundation for a successful security program.

In a cooperative effort with FTA, STSIP offers assistance to State Safety Oversight Agencies (SSOAs) in completing security audits of the Nation's 26 rail transit systems under 49 CFR 659, Rail Fixed Guideway Systems, State Safety Oversight.[167] This regulation, administered by FTA, requires rail fixed guideway[168] systems not regulated by FRA as a railroad to maintain a system security plan that meets specific parameters, conduct annual reviews of the plan, and conduct internal security reviews of the implementation and effectiveness of the security plan. The oversight agencies must ensure that transit systems under their responsibility conduct an annual review of their system security program plan.[169] Additionally, the oversight agencies must develop and document a process for conducting ongoing assessments of implementation of the system security program plan.[170] Covered rail transit systems must complete these assessments of all required elements of their system security program plan over a 3-year cycle. Each SSOA is required to perform an on-site review of implementation of the system security program plan at least every 3 years.[171]

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

[167] 49 CFR 659.
[168] 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.
[169] See id., 659.25.
[170] See id., 659.27.
[171] See id., 659.29.

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

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

Finally, TSA deploys STSIP inspectors to serve as Federal liaisons to mass transit and passenger rail system operations centers and provide other security support and assistance in periods of heightened threat or in response to security incidents. TSA initiated this component of the STSIP responsibilities in the aftermath of the attacks on the London transit system in July 2005. TSA inspectors are deployed to the operations centers of the transit systems in their areas to assess security response and serve as a liaison for information and coordination of resource support from the Federal Government. Since this initial deployment, inspectors have developed relationships with security officials in transit systems in their areas, coordinated access to operations centers, participated in or observed exercises, and provided other assistance consistent with the overall objective of enhancing security through collective effort.

3.2.2 National Explosives Detection Canine Teams

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

Figure Annex C3-4: The Initial 13 Systems Selected for Participation in NEDCTP

System Participation in NEDCTP	
• Massachusetts Bay Transportation Authority (MBTA) • San Francisco Bay Area Rapid Transit District (BART) • Southeastern Pennsylvania Transportation Authority (SEPTA) • Washington Metropolitan Area Transit Authority (WMATA) • Port Authority Trans-Hudson Corporation (PATH) • Dallas Area Rapid Transit (DART) • Tri-County Metropolitan Transportation District of Oregon (TriMet)	• Chicago Transit Authority (CTA) • Los Angeles County Metropolitan Transportation Authority (Metro) • Maryland Transit Administration (MTA) • San Francisco Municipal Railway (Muni) • San Diego Trolley, Inc. (SDTI) • Metropolitan Atlanta Rapid Transit Authority (MARTA)

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

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

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

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

3.2.3 Visible Intermodal Prevention and Response Teams

As part of implementing flexible, layered, and unpredictable security programs using risk management principles, this TSA program trains various teams, including law enforcement personnel, canine teams, and inspection personnel, for deployment to supplement mass transit and passenger rail system efforts to deter and protect against potential terrorist actions. The Visible Intermodal Prevention and Response (VIPR) teams provide TSA and the mass transit and passenger rail agencies with the ability to leverage a variety of resources quickly and effectively. Consisting of Federal Air Marshals, STSIP inspectors, TSA-certified explosives detection canine teams, and advanced screening technology, VIPR teams represent an ongoing effort to develop surge capacity to enhance security in public transportation systems. The teams work with local security and law enforcement officials to supplement existing security resources, provide deterrence and detection capabilities, and introduce an element of unpredictability to disrupt potential terrorist planning activities. These deployments enhance the agency's ability to leverage a variety of resources to raise the level of security quickly and effectively. By engaging regional, State, and local law enforcement and security entities as part of the VIPR teams, this program ensures robust sector participation.

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

Mass Transit Resource Center

TSA is working with OGT and FTA to develop the Mass Transit Resource Center, the application of the National Resource Center in the Public Transit portal of HSIN. The center provides a comprehensive database for the mass transit industry to access information on a broad spectrum of subjects pertaining to mass transit security, including material not readily available in a consolidated format elsewhere. TSA uses the portal to provide timely security alerts, advisories, and information bulletins to mass transit and passenger rail agencies. Technology updates constitute an important component of this resource. Overall, the center covers more than 20 subjects areas of security interest to the public transportation community, reflecting the feedback received from stakeholders on the type of information that they require to meet the security mission. The STSIP inspectors, through their various assessment programs, such as BASE and SAAP reviews, provide information on smart security practices for sharing among all mass transit and passenger rail systems. Additionally, TSA's Mass Transit Division will prepare and coordinate

through the interagency Mass Transit and Passenger Rail Security Information Sharing Network and the TCLDR-GCC, a periodic newsletter providing items on Federal transit security initiatives; recent suspicious activity reporting with the security context; and updates on model security practices observed in STSIP assessments, technology programs, and other areas of interest. This effort will also incorporate effective practices and items of general interest from mass transit agencies. Private sector input and feedback will be vital in shaping this resource to meet industry needs.

3.2.4 Information Sharing

Mass Transit and Passenger Rail Security Information Sharing Network

Effective information sharing is paramount to achieving the Transportation Systems SSP goals and objectives. A streamlined and effective system for sharing mass transit and passenger rail information is needed to facilitate information sharing among subject matter experts in the Federal Government and with public and private stakeholders. More efficient and timely information sharing will improve domain and situational awareness and allow the collaborative development of an agreed-upon common picture that Federal leadership can use to make well-informed and timely decisions.

In February 2002, FTA provided grant support to APTA to establish the Public Transit Information Sharing and Analysis Center (PT-ISAC), which operates a 24 hours per day, 7 days per week (24/7) information-sharing analysis center supported by analysts who cull through secure and open sources and communicate security-related information and advisories to public transit systems. Currently, more than 400 transit systems participate in the PT-ISAC. The PT-ISAC has both a Web-site analyst support and an electronic mail capability that can be used to share information with a broader audience. Somewhat similar are TSA and other agencies' communications tools (e.g., the DOT Crisis Management Center (CMC)), with the capability of using e-mail to pass along sensitive and non-sensitive information to stakeholders. All of these capabilities are important to maintaining a robust series of networks for the sharing of information between government and industry.

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

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

The Public Transit portal of HSIN is compatible with the DHS principles of sharing sensitive information over secure/encrypted lines. HSIN is a system where individual access is provided to users and is not available for the general public. It can be used in conjunction with the DHS alerts systems to notify users of the posting of critical information. TSA is working with OGT and FTA to integrate the National Resource Center into the Public Transit portal of HSIN as the Mass Transit Resource Center. The resource center will provide a comprehensive database for the transit industry to access information on a broad spectrum of subjects pertinent to transit security, including material not currently readily available in any consolidated format.

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

3.2.5 Security Training and Awareness Programs

Targeted Security Training Initiative

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

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

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

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

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

Connecting Communities

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

The MOU annex stipulates that TSA, FTA, and OGT host 12 Connecting Communities emergency response and preparedness training workshops to be provided through the National Transit Institute. These 2-day workshops enhance security and safety by sharing transit policies, procedures, resources, and effective practices with local first-responders, who would respond to transit emergencies, and discussing emergency management and response, including the role of Federal, State, and local emergency management offices to facilitate efficient planning, preparedness, and response coordination. In support of this regional engagement effort, area national JTTF representatives will provide presentations on their activities and coordination responsibilities. The most recent sessions of Connecting Communities occurred in the Washington, DC, metropolitan area in February 2007, and in Houston in March. Additional Connecting Communities forums will occur throughout 2007, consistent with the annex's goal of 12 sessions per calendar year. Coordination with the peer advisory group will foster achievement of this objective.

Safety and Security Roundtables

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

Federal Law Enforcement Training Center's (FLETC's) Land Transportation Anti-Terrorism Training Program

Transit employees, such as train conductors and bus drivers, can play a vital role in preventing a terrorist attack. In many cases, they will be in the best position to observe and report the suspicious activities that are the indicators of developing plans and operations. Effective reporting and coordination with law enforcement is essential. The Land Transportation Anti-Terrorism Training Program (LTATP) provides critical training to transit officials, local law enforcement, and others who have close, regular interaction with passengers. TSA funded eight of these programs through FLETC in FY 2006, and has made a similar commitment for FY 2007. The 1-week LTATP program is designed to enhance protection of land transportation infrastructure, including mass transit and passenger rail operations. The program is offered at eight different regional locations to maximize training opportunities for transit systems and affiliated law enforcement entities.

Transit Watch

The Transit Watch program, co-led by FTA and TSA, provides a nationwide safety and security awareness program designed to encourage the active participation of transit passengers and employees. By way of this program, the Federal Government, in collaboration with APTA, the Community Transportation Association of America, and the Amalgamated Transit Union, has created templates for transit agencies to develop and/or enhance their own public awareness programs. The templates that enable transit agencies to produce awareness materials, such as posters and flyers, with images and logos from their systems inserted, have been distributed nationally in a CD-ROM format. The materials are also accessible through the FTA and TSA public Web sites and the Public Transit portal of HSIN.

The See Something?, Say Something! campaign is derived from the Transit Watch program. Other materials include Employee Tip Cards, the Is This Your Bag? campaign, and a passenger rail pamphlet that includes information on how to deal with a security threat and monitor suspicious activities. The program employs a staged approach through basic and more advanced materials to boost public awareness and vigilance, adding a security force multiplier.

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

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

Random High-Visibility Passenger Awareness Program

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

The initial effort took place in 2006, in Washington, DC, near the fifth anniversary of 9/11, when the WMATA Metro Transit Police Department partnered with STSIP inspectors. TSA plans to offer this support throughout 2007, with the objective of conducting joint public awareness campaigns in eight regional areas.

Transit Terrorist Tools and Tactics (T4)

To enhance supervisory and frontline employee training and awareness, TSGP funded, and the University of Tenessee developed, the Transit Terrorist Tools and Tactics (T4) course. This intensive 3-day course provides participants with the knowledge, skills, and abilities to detect, deter, prevent, mitigate, and respond to the consequences of a terrorist CBRNE attack against a transit target. This course was offered to the mass transit community for the first time in fall 2006.

3.2.6 National Tunnel Security Initiative

This interagency effort brings together subject matter experts from a range of relevant fields among the DHS and DOT organizational elements to identify, assess, and prioritize the risk to mass transit systems in the United States with underwater tunnels, and to assist transit agencies in planning and implementing protective measures to deter and prevent attacks, and blast mitigation and emergency response strategies in the event of a terrorist attack and/or an all-hazards incident or event. Through regular meetings, this working group has developed mitigation strategies; engaged stakeholders; analyzed and applied

the results of risk assessments; prepared statements of work for testing and modeling programs; and integrated the overall risk mitigation effort into a cohesive, coordinated, and effective approach. The initiative has:

- Identified and assessed the risks to underwater tunnels;
- Prioritized tunnel risk mitigation based on risk to drive grant funding to the most pressing areas;
- Developed strategies for funding future technology R&D aimed at producing novel approaches to this challenging problem; and
- Produced and disseminated recommended protective measures that transit agencies may implement to enhance security with available resources or through targeted grant funding.

To advance this concerted effort, TSGP makes projects to protect high-risk underwater and underground assets and systems a top funding priority.

3.2.7 Security Technology Deployment

This cooperative initative between TSA and mass transit and passenger rail stakeholders deploys various security technologies to interested public transportation systems for security supplemental and developmental testing. The program introduces the stakeholders to new technology, assists with their screening needs, and conducts surge operations around the United States. A formal process led by the DHS Science and Technology Directorate (S&T) and the TSA Chief Technology Officer], 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 technology deployment.

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

3.2.8 Technology Research and Development

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

Through the Transit Safety and Security Roundtables discussed earlier, stakeholder tours of S&T's Transportation Security Laboratory, interagency informational tours, and other meetings, TSA and its Federal partners exchange information on planned research, development, test, and evaluation (RDT&E) efforts; projects; and needs and challenges with the stakeholders and scientific and technology communities. The results are developed into broad requirements submitted to S&T for R&D. Furthermore, TSA participates in the Integrated Project Teams (IPTs) held by S&T across a variety of critical infrastructure and potential threats. These IPTs provide a means to submit technology requirements for funding and coordinate requirements with other DHS internal stakeholders (i.e., Customs and Border Protection (CBP), the U.S. Coast Guard) to eliminate duplication of effort and share experience and knowledge. TSA and industry representatives also participate in bilateral and multilateral international meetings and working groups on technology that focus on the sharing of information on a specific technology or broad technology needs and requirements. TSA and its partners are working on a plan to utilize the HSIN Public Transit portal

as a tool to provide government and industry with a list of available technologies and products related to the protection of mass transit and passenger rail.

Improved Mass Transit Surveillance and Early Warning System

This R&D project entails developing software analytics to identify human anamolous and suspicious behavior using new and legacy surveillance camera systems. The first phase of testing is occurring in two light rail stations in the Metro Transit system in Minneapolis. The second phase will take place at the Amtrak® 30th Street Station in Philadelphia.

Bus Communications and Control

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

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

Moveable Security Checkpoints

TSA has conducted field testing on a Moveable Security Checkpoint. This mobile equipment, which can fit into two standard-sized shipping containers, can be rapidly deployed for use in screening and detection at any major system in the country. The equipment has performed effectively in Maryland in the MARC commuter rail system and the Maryland Transit Administration light rail system. This is another tool available for deployment at mass transit and passenger rail locations throughout the Nation randomly; in the event of a threat, incidient, or natural disaster; and during national security special events. TSA has dedicated funding to support deployment of these checkpoints.

National Capital Region Rail Security Corridor Pilot Project

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

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

Bomb-Resistant Trash Cans

OGT's Systems Support Division has conducted operational tests to evaluate manufacturer's claims on ballistic-resistant trash receptacles and has published a report on its findings to help ensure that mass transit and passenger rail systems, among others,

have the information needed to guide critical procurement decisions. Similarly, the Systems Support Division has published a Closed-Circuit Television (CCTV) Technology Handbook to provide a reference point on current CCTV technologies, capabilities, and limitations.

3.2.9 International Initiatives

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

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

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

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

Another international initiative focuses on vetting suspicious packages detected in transit systems. This joint effort, involving STSIP inspectors, Los Angeles law enforcement representatives, and British security officials, will bring training, experience, and lessons learned to American participants from a British program for dealing with suspicious packages, known as Hidden, Obviously Suspicious, and Not Typical (HOT). This program enhances the ability of trained personnel to identify indicators of security concerns with packages left unattended in transit and rail facilities and vehicles.

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

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

3.3.1 Security Guidelines

In the immediate aftermath of the terrorist attacks against the United States on 9/11, FTA took steps to enhance security postures and practices among transit systems nationwide. FTA established 20 specific action items (the top 20) for transit system security readiness. The action items and supporting references provided an excellent resource to facilitate the development of security plans and programs. FTA used the top 20 as an assessment tool to determine the readiness of the Nation's 50 largest transit agencies (the results were indicated by a red/yellow/green stoplight chart depicting the transit agency's posture in each of the recommended action items), as part of its technical assistance program to the 50 largest transit agencies. FTA also used the top 20 assessments as a gap analysis tool, identifying areas where transit agencies needed additional guidance. Gap analysis

products include a threat level protective measures guidance document discussed below, which was recently updated by FTA and TSA.

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

Through the BASE program, STSIP inspectors assess a transit system's security posture on the 17 SAIs, with a particular emphasis on 6 core transit security fundamentals, discussed in more detail in section 3.5. The BASE program aims to elevate security generally and expand TSA's awareness and understanding of security postures in the Mass Transit and Passenger Rail Mode. This information enables more effective targeting of security programs and technical assistance to elevate security. Through this process, TSA also identifies best security practices for sharing with the mass transit and passenger rail community, further enhancing security postures. This thorough review of security programs and procedures affords the systems assessed the opportunity to review the state of their security program and identify strengths and weaknesses. This information can guide the effective application of available security resources, focus collaborative efforts with TSA, and facilitate the preparation of funding requests through security grant programs.

Another jointly developed product by TSA and FTA, also coordinated with the Mass Transit SCC, is the recommended protective measures for the threat levels under the HSAS. This product is an update of the Transit Threat Level Response Recommendation product developed by FTA to provide guidance to the U.S. transit industry in responding to the threat level designations set by the then Office of Homeland Security. The current recommended protective measures reflect the advantages of improved threat and intelligence information, security assessments conducted by FTA and TSA, operational experience since the 9/11 attacks that prompted the original version, and the collective subject matter expertise and experience of Federal partners and the transit community. This product has been developed as a technical resource for transit agency executive management and senior staff assigned to develop security and emergency response plans and implement protective measures for response to the HSAS threat conditions and emergencies that might affect a transit agency. The updated protective measures may be accessed at the Public Transit portal of HSIN.

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

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

3.3.2 Security Standards Development

The Federal Government is engaging with the APTA Security Standards Policy and Planning Committee to develop security standards. In transit safety, APTA has been actively involved in transit industry standards development for more than 9 years and is recognized by the Federal Government and other standards organizations as a "Standards Development Organization."

The security standards development effort brings together security professionals from the public transportation industry, business partner representatives, and the Federal Government in a collaborative effort to develop consensus-based standards to enhance security in transit systems. Federal participants consist of subject matter experts from OGT, TSA (Mass Transit Division and STSIP), FTA, and FRA. Public transportation stakeholder participants consist of members of the APTA Security Standards Policy and Planning Committee, officials from mass transit and passenger rail systems, and industry businesses and research organizations. Working groups are established to focus on specific security areas and concerns, including mass transit and passenger rail systems, facilities, and operations.

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

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

3.3.3 Security Directives

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

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

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

3.3.4 Notice of Proposed Rulemaking

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

threats or significant security concerns to TSA's Transportation Security Operations Center (TSOC).[172] The draft rule also details TSA's authority concerning inspection of the facilities and operations of covered passenger rail and rail transit systems and hosts of passenger rail service.

This NPRM provided ample time for comments by stakeholders and the public at large. A public meeting was held on February 2, 2007, to provide further opportunity for comments. TSA is reviewing the comments and making the appropriate changes, if any, to the proposed rule.

3.4 Grant Programs

Through TSGP, the DHS has allocated $547 million to date to 60 of the Nation's mass transit and passenger rail systems in 25 States and the District of Columbia. TSGP employs risk-based prioritization consistent with the Transportation Systems 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 the ability to reduce risk, cost-effectiveness, and the ability to complete the proposed project with the funds awarded.

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

The application of risk-based priorities is being institutionalized by developing a regulation governing TSGP. Mandated under SAFETEA-LU,[173] the DHS and DOT will jointly issue the rule. The draft rule places particular emphasis on ensuring that transit systems enhance their capabilities in implementing six core transit security fundamentals that provide the essential foundation for effective security programs:

1. **Protection of high-risk underwater/underground assets and systems.** Because of the consequences of IED attacks in an enclosed environment where there may also be large concentrations of riders, protecting riders and the integrity of the transit system against such attacks is essential. Transit agencies should focus countermeasures on programs that can prevent an attack or mitigate the consequences of an incident. Active coordination and regular testing of emergency evacuation plans can also greatly reduce loss of life.
2. **Protection of other high-risk assets that have been identified through system-wide risk assessments.** It is imperative that transit agencies focus countermeasure resources on their highest risk, highest consequence assets. For example, a system-wide assessment may highlight the need to segregate critical security infrastructure from public access. One solution could be an integrated intrusion detection system, controlling access to these critical facilities or equipment. Transit systems should consider security technologies to help reduce the burden on security manpower. For example, using smart CCTV systems in remote locations can help free up security patrols to focus on more high-risk areas.

[172] These requirements are currently included in Security Directives RAILPAX-04-01 and RAILPAX-04-02.
[173] Safe, Affordable, Flexible, Efficient Transportation Equity Act: A Legacy for Users, Public Law 109-59, August 10, 2005.

3. **Use of visible, unpredictable deterrence.** Visible and unpredictable security patrols have proven to be very successful for instilling confidence and calm in the riding public and, most importantly, in deterring attacks. These kinds of patrols, especially those employing explosives detection canine teams or mobile screening or detection equipment, represent effective means to prevent or deter IED attacks. Security patrols should be properly trained in counterterrorism surveillance techniques. An understanding of terrorist behavior patterns helps security patrols more effectively intervene during terrorist surveillance activities or the actual placing of an IED.

4. **Targeted counterterrorism training for key frontline staff.** Appropriate training enhances detection and prevention capabilities and ensures a rapid, prepared response in the first critical minutes after an attack—steps that can significantly reduce the consequences of the attack. For example, well-trained and well-rehearsed operators can help to ensure that if an underground station has suffered a chemical agent attack, trains—and the riding public—are quickly removed from the scene, thus reducing their exposure and risk.

5. **Emergency preparedness drills and exercises.** Experience has taught transit agencies that well-designed and regularly practiced drills and exercises are fundamental for rapid and effective response and recovery. Transit agencies should develop meaningful exercises, including covert testing, that test their response effectiveness and how well they coordinate with first-responders. In addition to large regional drills, transit systems should also conduct regular, transit-focused drills. Drills should test response and recovery to both natural disasters and terrorist attacks.

6. **Public awareness and preparedness campaigns.** Successful security programs in all industries understand the value and power of the public's eyes and ears. Awareness programs should be well-designed and employ innovative ways to engage the riding public to become part of their "transit security system." Advertisement campaigns, using media and celebrity support, have proven to be very successful. Including the riding public in preparedness and evacuation drills has also been shown to be effective in raising public awareness. A transit agency's awareness campaign should also extend to its employees. Appropriate counterterrorism training, coupled with a strong security awareness campaign, will yield significantly heightened security awareness in transit systems.

3.5 The Way Forward

The Federal Government recognizes the value of consensus-based decisionmaking at every level of engagement with the public transportation industry to develop strategies and programs for enhancing security postures and practices throughout the mode, while complying with applicable legal requirements. A major step in the process is being reached through the TCLDR-GCC and the Mass Transit SCC and through the CIPAC process at the national level. This process facilitates coordination on developing security strategies, programs, and initiatives, and allows for more effective execution of Executive Order 13416, Strengthening Surface Transportation Security, the successful implementation of which would not be possible without collective engagement and consensus-based decisionmaking.

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

TSA is leading the formation of regional public transportation GCCs and encouraging public transportation stakeholders in metropolitan areas throughout the United States to form regional SCCs. These councils will foster development and communication of coordinated policies and positions on matters of transportation security and operational efficiency. Members of the

respective councils would engage in collaborative efforts to develop and implement security strategies, plans, and programs under CIPAC.

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

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

- TSA (Federal Security Director or designee, STSIP inspectors, Federal Air Marshals);
- DHS officials serving in the area, if available (such as a DHS Protective Security Inspector or representatives of CBP and/or Immigration and Customs Enforcement (ICE));
- Regional DOT personnel (such as FRA field inspectors and FTA regional office representatives);
- The U.S. Coast Guard detachment in the area, if applicable;
- SSOA representative;[174]
- State Homeland Security Advisor, county or local homeland security officials;
- FBI's national JTTFs and other Federal, State, tribal, and local law enforcement entities with jurisdiction in the area; and
- Other governmental first-responders, such as any fire departments in the area.

The developing model framework encourages such initiatives and aligns their development and implementation with the public-private partnership model envisioned under HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection, and effected by the NIPP and the Transportation Systems SSP. This approach calls for the establishment of regional transportation GCCs in areas where TSA security officials are assigned. The Federal Security Director or his designee, such as an Area Director for the Surface Transportation Security Inspection Program, engages the area Federal, State, and local government officials responsible for transportation security. The following are the benefits of such regional GCCs:

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

These regional GCCs should encourage transportation stakeholders to form regional SCCs. Neither an individual government agency nor a regional GCC may direct the formation of a regional SCC; however, governmental entities may encourage such organizing to facilitate collaborative efforts on the full spectrum of security issues.

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

[174] Designated per 49 CFR 659.

3.6 Metrics

General

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

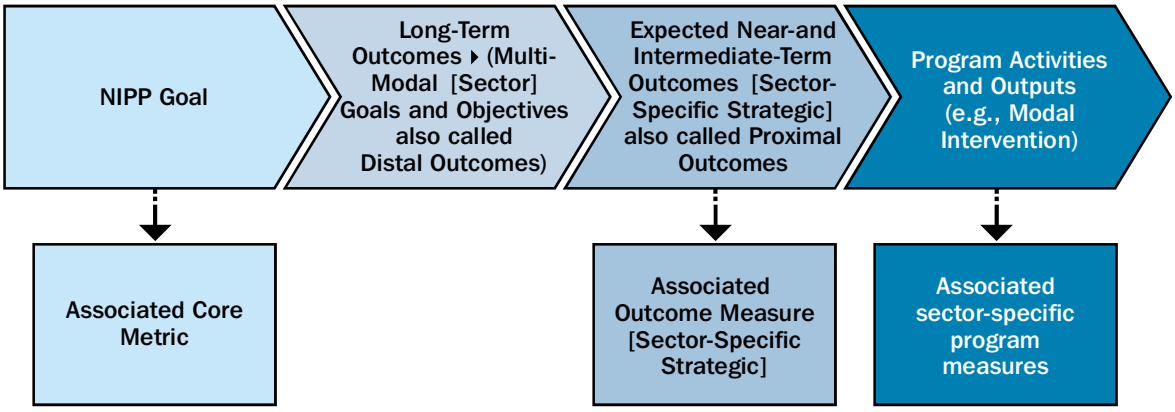
Measurement Joint Working Group

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

Measures

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

Figure Annex C3-5: Outcome Model



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

1. **Core.** Core NIPP metrics are common across all sectors and focus on measuring risk-reduction progress in the sector. These measures are often descriptive statistics (counts). The following is an example of mass transit and passenger rail NIPP core metrics: Number of mass transit assets/systems/networks that have performed a vulnerability assessment.
2. **Sector-Specific Strategic.** These metrics are used to gauge the overall effectiveness of the Mass Transit and Passenger Rail Mode and other modes toward meeting Transportation Systems SSP goals and objectives. Ordinarily, these are outcome measures capable of quantifying the degree to which the SSP is affecting sector security. In the early stages of the program,

substitute output measures may need to serve as proxies for the long-term outcome measures. In this instance, output data are likely to be collected from the mode and combined at the sector level (or reported independently at the mode level).

3. **Sector-Specific Program.** These measures are aligned to the strategic risk objectives (i.e., priorities, strategies, etc.) for the Transportation Systems Sector. Strategic risk objectives for the sector will be developed consistent with the discussion in section 3 of the Transportation Systems SSP Base Plan. Strategic risk objectives are developed with program measures and should be aligned to the overall Transportation Systems SSP goals and objectives. Standard performance measurement techniques for mass transit and passenger rail programs will be supplemented with measures to demonstrate how the program is meeting associated Transportation Systems SSP strategic risk objectives.

4 Program Management

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

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

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

The business plan further stipulates the following:

Communications/Information Sharing

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

Security Guidelines and Standards Development

- TSA and FTA, in coordination with the Mass Transit SCC, will regularly review and, as necessary, update the SAIs and the HSAS Recommended Protective Measures. This dynamic approach will ensure that these products continue to address current risks and reflect the most effective baseline security measures and practices. As part of this effort, TSA and FTA will conduct an evaluation of the results of security assessments to develop specific recommendations on effective security measures and practices.
- TSA will work with the TCLDR-GCC, the Mass Transit SCC, and the Transit Policing and Security Peer Advisory Group, within the context of CIPAC, to continue to advance the development of security standards, potentially integrating a tier-based program. This program may model the National Law Enforcement Accreditation Program. The security standards program will include a self-assessment module.
- TSA will continue to offer security assessments by STSIP inspectors under the BASE program to review mass transit and passenger rail systems' security postures with regard to the 17 SAIs. The assessment checklist may also be provided to systems for the conduct of self-assessments in advance of an STSIP-led review and to guide internal security audits. Additionally, working through the Transit Policing and Security Peer Advisory Group, TSA will coordinate conduct of self-assessments by the top 50 transit agencies on the 6 transit security fundamentals.
- Where self-assessments are conducted, STSIP inspectors will follow up to verify the results and engage in an informed discussion on the systems' security postures based on the NIPP's risk assessment principles.
- TSA will consult with the Transit Policing and Security Peer Advisory Group under the CIPAC process to establish model security practices and guidelines similar to the APTA/FTA security guidelines manual.

Training

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

Security Technologies and Research and Development

- Through the Mass Transit Security Technology Working Group, formed under the auspices of the Public Transportation Annex to the DHS/DOT MOU, TSA, FTA, and OGT will work with the Mass Transit SCC and the Transit Policing and Security Peer Advisory Group, employing the CIPAC process, as necessary, to develop a priority R&D action plan.

- TSA, FTA, and OGT will establish a Web-based information resource on operating standards and specifications for security technologies. This effort includes establishing priorities to ensure the availability of information on existing technologies in the most expeditious manner and leveraging testing work already completed and databases, such as the OGT SAVER network, already developed.
- TSA and the Transit Policing and Security Peer Advisory Group will establish a database of technologies deployed by various transit systems. This information will facilitate networking and sharing of lessons learned among mass transit and passenger rail systems to enhance the employment of security technologies.
- TSA, working with S&T, will establish and conduct pilot testing to advance the development of flexible security solutions and enhance deterrence through visible, random, and unpredictable employment of security technologies.

5 Mass Transit and Passenger Rail Security Gaps

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

This information is, in part, derived from the data generated using the results of the BASE program reviews completed to date by STSIP and reflects the current implementation status of the transit security fundamentals and the FTA/TSA SAIs.

1. Information Sharing

There are two security gaps in information sharing:

- Not all of the top 100 transit agencies have enrolled in HSIN; and
- There is currently an inability to disseminate such material to properly cleared transit agency officials in a timely manner.

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

2. Employee Security Training

The findings of the BASE program indicate that while many transit agencies provide initial anti-terrorism training to their employees, adequate refresher training is not being provided. Furthermore, the findings indicate that security orientation and awareness training, as well as emergency response training, is not adequately reinforced. Gaps in training in these and other areas, such as agency-developed incident response protocols, incident commend systems, the National Incident Management System, and IEDs/weapons of mass destruction, are being addressed through the development of a Mass Transit Security Training Program and 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, along 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 TSGP. Transit agencies request particular types of training for the various categories of employees. Grant awards cover the cost of training and overtime or related expenses to backfill employees in classes. TSA is committed to expedited processing to get funds to the transit agencies.

3. Security Awareness Campaigns

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

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

4. Research and Development and Technology Deployment

R&D is needed to close or mitigate known 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 laboratories in the Federal and national system to conduct these tests.

In this area, there is also a need for expedited means to identify and test explosives detection devises 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 infrared capabilities and alert systems that identify anomalous behavior or objects.

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

5. Mitigation Strategies for Underwater/Underground Tunnels

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

6. Drills and Exercises

Broader effort is necessary to engage regional security partners (area law enforcement agencies and fire and emergency response units) to ensure thorough familiarity with the operating environment, interoperable communications capabilities, and development of coordinated command and control. The results of the BASE program reviews indicate that transit agencies are generally doing well in conducting drills and exercises. More effort is needed in leveraging the national exercise and drill capabilities developed at the 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 is a strategic priority for TSA.

Annex D. Highway Infrastructure and Motor Carrier

1 Executive Summary

The Highway Infrastructure and Motor Carrier Modal Annex to the Transportation Systems Sector-Specific Plan (SSP) describes how Transportation Systems Sector goals and objectives will be achieved to protect what is referred to as the Highway Transportation System. These assets include, but are not limited to, signature bridges, major tunnels, operations and management centers, trucks carrying hazardous materials (HAZMAT), other commercial freight vehicles, motorcoaches, schoolbuses, and key intermodal freight transfer facilities.

While the in-vehicle and highway facilities infrastructure optimizing the movement of people, services, and cargo through the Highway Transportation System are robust, some are essential in facilitating Federal and State services to maintain the health of the public, economic vitality, telecommunications, electricity, and other essential services. Even temporary debilitation of a bridge or tunnel could result in regional shutdowns, diversions, or costly repairs with potentially severe results. The security of the Highway Transportation System is a shared responsibility among Federal, State, and local governments and private stakeholders. Measures to secure the assets of the Highway Transportation System must be implemented in a way that balances cost, efficiency, and preservation of commerce in this Nation. The Highway Infrastructure and Motor Carrier Annex will require periodic updates to reflect current conditions, enhanced strategies, new programs, and Government Coordinating Council (GCC)/Sector Coordinating Council (SCC) scope of planning for the following year. Federal, State, local, and tribal government agencies, along with private stakeholders, will lead the national effort to maintain the capability to move freely and facilitate interstate commerce under all conditions.

Vehicles that use the highways are potential targets and weapons that terrorists or criminals could use to attack critical infrastructure or other assets. The trucking industry is unique in that it is the only segment of the Highway Infrastructure and Motor Carrier Mode with complete intermodal supply chain relationships with the Aviation, Maritime, Mass Transit and Passenger Rail, Freight Rail, and Pipeline modes. The bus industry, similar to the trucking component, also operates with multi-modal interconnectivity on a daily basis, 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.

To address these security issues, it is important that the Federal Government continues to work effectively within the established public-private partnership to implement a variety of programs to enhance the security of domestic highway operations. Highway infrastructure and motor carrier security is advanced by implementing layered security measures into transportation systems operations and management. Toward this end, the Department of Homeland Security (DHS), the Department of Transportation (DOT), State and local government entities, and the private sector security partners continue to be committed to improving the Highway Transportation System. Technology and human capabilities must keep pace with the increasingly sophisticated terrorist or criminal techniques that may be used to threaten the Highway Transportation System or its components.

2 Overview of Mode

The physical components of the Highway Transportation System include the following basic features: infrastructure, vehicles, users, equipment, facilities, control/communications, and facilities.

Infrastructure, the "fixed" part of the system, includes roads, bridges, tunnels, and terminals where travelers and freight can enter and leave the system. Many vehicle types operate on the highway system, moving both people and freight. The users include commercial vehicle and private passenger drivers, cargo shippers and receivers, passengers, and pedestrians. Equipment refers to the maintenance machinery that operates to facilitate transportation. Facilities refer to the terminals, warehouses, depots, and other transportation-related buildings. Finally, control and communications are methods for controlling vehicles, infrastructure, and entire transportation networks. These methods include both humans and the application of technology to improve Highway Transportation System security and operations.

2.1 Vision of Mode

The vision of the Highway Infrastructure and Motor Carrier Mode is to lead the national effort to maintain the capability to move freely and facilitate commerce under all conditions, and to continuously set the standard for excellence in highway transportation security through our people, processes, and technology.

2.2 Description of Mode

The Nation's Highway Transportation System is robust and interconnected, including 3.8 million miles of roadway; 582,000 bridges; and 54 tunnels more than 500 meters in length. Significantly, the highway system supports 86 percent of all of our citizens' personal travel, moves 80 percent of the Nation's freight (based on value), and serves as a key component in national defense mobility. Despite widespread redundancies, there are critical junctures with limited capacity for additional traffic. Freight volume is projected to double by 2020, stretching the Nation's ability to manage limited capacity and growing security concerns.

Addressing potential threats to the highway system is particularly challenging because of the openness of the system. Vehicles and their operators move freely in the system, with almost no restrictions. Some bridge and tunnel elements are especially vulnerable because many structural elements are accessible and in isolated locations. State and local governments own most highways, although independent entities own some major, iconic structures. Protecting the Highway Transportation System is a shared responsibility between State and local transportation agencies and their sister agencies responsible for law enforcement. This reality is important when considering the potential costs of heightened security measures.

The trucking industry is made up of predominantly small private companies. Approximately 675,000 are interstate and 400,000 are intrastate companies. In addition to for-hire trucking, private truck operations are integral to other business operations, such as construction, agriculture, and the delivery of goods and services. Nearly 8 million large trucks are registered in the United States. While approximately 9.3 million truck drivers have commercial driver's licenses (CDLs), only 3.3 million are regarded as active. Vehicle configurations include tankers, dump trucks, intermodal containers, flat-beds, and specialty vehicles.

Trucks transport the majority of all of the goods in the United States. These shipments include agricultural goods, hazardous materials (HAZMAT), electronics, and automotive and other products essential to our economy. The trucking industry is unique in that it is the only segment of the Highway Infrastructure and Motor Carrier Mode with complete intermodal supply chain relationships with the Aviation, Maritime, Mass Transit and Passenger Rail, Freight Rail, and Pipeline modes. With widespread access to not only intermodal infrastructure, but also contact with large numbers of people and goods, it is important that coordination between trucking operation and other modes include effective lines of communication and coordinated security measures to establish and maintain safe and secure transport of goods and people.

The motorcoach industry is comprised of approximately 3,600 motorcoach companies, operating 39,000 motorcoaches that carry nearly 630 million passengers annually in the United States and Canada, traveling approximately 2.44 billion miles per year. The motorcoach industry, similar to the trucking component, also operates with multi-modal interconnectivity on a daily basis, providing passenger and limited freight service on a national level. Again, such open access requires coordinated safety and security efforts across modes.

The school transportation industry, which is comprised of approximately 460,000 schoolbuses, is the largest public fleet of vehicles in the United States. Each day, nearly 23.5 million minor students travel to approximately 14,000 public educational agencies nationwide. In the United States, schoolbuses travel 4 billion miles annually on fixed daily routes, as well as periodically conducting transportation to public venues.

2.3 GCC/SCC Structure and Process

Objective

The National Infrastructure Protection Plan (NIPP) calls for forming a Government Coordinating Council (GCC) and a Sector Coordinating Council (SCC) to provide a forum for coordination and information exchange.

The objective of the Highway Infrastructure and Motor Carrier Modal GCC (hereinafter referred to as the Highway GCC), is to coordinate highway and motor carrier security strategies and activities; establish policies, guidelines, and standards; and develop program metrics and performance criteria for the mode. The Highway GCC fosters communication across government agency lines and between the government and private industry in support of the Nation's homeland security mission. It also functions as the counterpart to the private industry-led Highway Infrastructure and Motor Carrier Modal SCC (hereinafter referred to as the Highway SCC) to review and develop the security programs necessary to protect the Nation's Highway Infrastructure and Motor Carrier Mode.

Scope of Activity: GCC

The Highway GCC will address highway infrastructure, commercial vehicle operations, and supporting facilities using the risk-based methodology delineated in the NIPP and the Transportation Systems Sector-Specific Plan (SSP). The Highway GCC will accomplish this objective through the following activities:

Information-Sharing Mechanisms

The Highway Infrastructure and Motor Carrier Mode has the Highway Information Sharing Analysis Center (ISAC) and the Homeland Security Information Network (HSIN) as two mechanisms for sharing information with the highway industry.

- **Highway ISAC:** The American Trucking Associations (ATA) operates the Highway ISAC in partnership with the national and State trucking associations and conferences of the ATA Federation, and numerous other national highway transportation organizations in the Highway Watch® Coalition, in cooperation with the Department of Homeland Security (DHS) for the benefit of the entire Highway Transportation System.

  The Highway ISAC disseminates information bulletins, alerts, and other security-related reports to stakeholders via e-mail. The ISAC works with both public and private stakeholders to collect, share, and analyze information that provides a security benefit for the Highway Infrastructure and Motor Carrier Mode.

- **HSIN:** The HSIN is intended to be a secure, single-source, information-sharing Web-based network to assist in the two-way communication of security-related information. The Highway GCC has created a Web portal on HSIN. In addition, the Highway SCC will be creating their own Web portal on HSIN to allow private sector stakeholders to engage in two-way communication with the public sector to share, review, discuss, and disseminate security information in an efficient and effective format.

Framework to Address Critical Issues

The Highway GCC and SCC coordinate on projects involving policies that advance modal security. They may also meet to identify issues and provide recommendations or reports to the Transportation Systems Sector GCC, as necessary.

Membership

The Highway GCC membership consists of key Federal departments and agencies responsible for or involved in highway and motor carrier security. This membership may be expanded to include State and local officials with an interest in the Highway Infrastructure and Motor Carrier Mode.

The Highway GCC 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 the appropriate levels of government and with private industry.

The Highway GCC will add permanent Federal department or agency members, as deemed necessary and appropriate. The Highway GCC will invite ad hoc members with special expertise from other departments, agencies, or offices from time to time to meet the expertise requirements necessary to fulfill its mission.

The following are member organizations of the Highway GCC:

- 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 Energy
- Nuclear Regulatory Commission
- DHS Customs and Border Protection
- DHS Office of Infrastructure Protection
- DHS Homeland Infrastructure Threat and Risk Analysis Center
- DHS National Preparedness Directorate
- DHS Office for State and Local Government Coordination
- American Association of State Highway and Transportation Officials
- Commercial Vehicle Safety Alliance
- American Association of Motor Vehicle Administrators
- International Association of Chiefs of Police
- National Sheriffs' Association
- Federal Bureau of Investigation

Scope of Activity: SCC

Private sector owners and operators and representative associations of highway and motor carriers assets have formed a Highway SCC to partner with senior government officials to collaborate and communicate on security initiatives designed to enhance the protection of Transportation Systems Sector critical infrastructure and key resources (CI/KR). The Highway SCC is an industry advisory body that, as appropriate, will coordinate the private industry perspective on highway and motor carrier security policy, practices, and standards that affect the Transportation Systems Sector.

The Highway SCC will operate in a similar manner to the GCC described above. It includes members from the motorcoach, schoolbus, and trucking industries, and related associations. Many of the members are either an association representative or an employee for a private company in the highway transportation industry.

The objectives of the SCC are to:

- Facilitate intra-sector communications, set processes for information sharing, and facilitate priority setting on sector strategy and planning, policies and procedures, threat communication and analysis, as well as sector protection, response, and recovery planning and activities;
- Serve as an interface with the DHS and other Federal and State agencies on homeland security matters;
- Facilitate communications, plans, and activities with other relevant infrastructure sectors, government entities, and others necessary to further secure the Nation's highway and motor carrier critical infrastructure assets; and
- Communicate the sector's needs and requests for resources to the Highway GCC.

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 Associations
- Border Trade Alliance
- 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
- 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
- United Motorcoach Association

3 Implementation Plan

3.1 Priorities and Programs

3.1.1 Priorities

The mission of the Transportation Systems Sector is to continuously improve the risk posture of the national transportation system using a risk management framework. The Transportation Systems SSP identifies a number of goals for enhancing security in the Transportation Systems Sector.

Goals

- Prevent and deter acts of terrorism using or against the transportation system;
- Enhance the resilience of the transportation system; and
- Improve the cost-effective use of resources for transportation security.

The public sector has developed a number of critical voluntary and mandatory programs that incorporate elements to target and assess risk, and secure the Highway Transportation System. Many of these efforts encourage private sector initiatives in security and increase the government's visibility in the Highway Transportation System without disrupting the movement of cargo or people. Many programs of the Federal Government are currently focused on security awareness training, technology, and screening programs. These programs seek to develop common security practices to mitigate security risks. Some government-led efforts are outlined below.

The sector has identified ways to achieve these goals, including: (1) the standardization of risk assessment and risk mitigation approaches; (2) the establishment of performance-based security guidelines through collaboration with stakeholders; (3) the integration of security measures into the design of the Nation's transportation network; (4) the use of existing security grant

programs; (5) development and adoption of security technology; (6) enhancement of driver threat assessments and credentialing; (7) enhancement of existing HAZMAT security requirements; and (8) enhancement of owner/operator and law enforcement awareness and training. A description of key priorities and program details follows. The programs described below are designed to implement more than one goal or objective although they are discussed here under their primary objective.

3.1.2 Sector Goals and Objectives

Goal 1: Prevent and deter acts of terrorism using or against the transportation system.

Objectives

Implement flexible, layered, and effective security programs using risk management principles. The highway sector will develop and implement layered security programs using risk management principles (discussed in sections 3 through 7 of the Transportation Systems SSP). Sustained focus on the following risk-based priorities for the highway infrastructure and motor carrier industry will reduce vulnerability and minimize the consequences of a terrorist attack, while also improving the efficiencies of this important and complex transportation network.

- **Standardize Risk Assessment and Risk Mitigation Approaches.** Coordinated communication between the public and private sectors will assist in making informed decisions on the use of limited resources in the areas of greatest risk. The Federal Government will continue to partner with the private sector to improve the risk assessment system that all highway stakeholders within similar industry disciplines can use to identify risk, based on threat, vulnerability, and consequence. This task involves identifying each major segment of the Highway Transportation System structural, conveyances, systems, and personnel, and the specific aspects, vulnerabilities, and mitigation strategies common to all and unique to each. Federal partners will work to develop assessment and mitigation solutions for each. The Transportation Security Administration (TSA), the Federal Motor Carrier Safety Administration (FMCSA), and the Federal Highway Administration (FHWA) are currently working to combine their individual risk assessment and risk mitigation tools into one document that will reduce redundancy, increase efficiencies, and minimize the impact on private stakeholders.

- **Corporate Security Review (CSR) Program.** CSRs are conducted with organizations engaged in transportation by motor vehicle and those that maintain or operate key physical assets within the highway transportation community. They serve to evaluate and collect physical and operational preparedness information, and critical asset and key point-of-contact lists; review emergency procedures and domain awareness training; and provide an opportunity to share industry best practices.

- **Security Action Items (SAIs).** Consistent with Executive Order 13416, Strengthening Surface Transportation Security, TSA is drafting SAIs that are voluntary practices designed to improve security for trucks carrying security-sensitive HAZMAT, motorcoaches and schoolbuses, and highway infrastructure. These SAIs are being coordinated with the Department of Transportation's (DOT's) FMCSA and FHWA. Once the SAIs are completed, the Highway SCC will solicit and obtain industry review and input on the SAIs prior to issuance. SAIs, though voluntary, will allow TSA to communicate and share formally with applicable stakeholders those security actions identified as key elements within an effective and layered approach to transportation security. Many of the applicable stakeholders are currently employing some of these security actions as evidenced by the results of the CSRs.

  The Federal Government will work with highway stakeholders to identify and establish measurable SAIs. Performance-based standards provide highway asset/system owners and operators the flexibility to tailor approaches to each facility's unique risks and configurations; they could include standards for enhancing physical and cyber security, including surveillance detection, escalating perimeter/access controls for heightened alert status, and structural hardening. The Federal Government will also work with the private sector to develop a catalog of highway-specific protective measures that correspond with the Homeland Security Advisory System (HSAS) levels, and apply existing best practices. Furthermore, FHWA and TSA are work-

ing with State DOTs to incorporate security programs as part of their all-hazards approach to emergency planning, preparedness, and response.

- **FHWA Security Self-Assessment Tool.** FHWA's Security Self-Assessment Tool assists their field offices in working with their State DOT counterparts to: (1) assess the current state of highway transportation security, and (2) identify potential areas for improvement. This tool consists of a discussion paper, entitled "Attributes of an Effective State Highway Asset Security Program," and a checklist to use in assessing the current state of the practice. The intent is to review State security processes and procedures on a 2-year cycle to ensure that State programs keep abreast of changes in security conditions, identifying program areas for improvement and monitoring progress.

Increase the vigilance of travelers and transportation workers. By having an active role in identifying and reporting suspicious activities, the traveling public and transportation workers can serve as force multipliers to Federal, State, and local law enforcement efforts.

- **Enhance Owner/Operator and Law Enforcement Awareness and Training.** The Federal Government will work closely with industry stakeholders, and State, local, and tribal governments to enhance truck and motorcoach awareness and training. Existing Federal site visit programs will be coordinated to enhance security awareness and training, and provide technical and threat information. This effort will build on existing complementary DHS and DOT efforts. The Federal Government will also provide assistance to the bus and motorcoach industries to develop and implement security plans and security training for employees. Enhancing programs that support law enforcement agencies, such as DOT's Trucks 'n Terrorism training and courses offered by the DHS's Federal Law Enforcement Training Center, will raise awareness of indicators of suspicious activities involving commercial motor vehicles.
- **Consolidate Driver Threat Assessments and Credentialing Programs.** Congress passed the REAL ID Act in 2005 (Division B of an act entitled Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief). The DHS issued a Notice of Proposed Rulemaking in March 2007 that proposes to significantly enhance the security of the issuance of State driver's licenses.

  The DHS requires all individuals who receive, renew, or transfer a HAZMAT endorsement for a CDL to successfully complete a rigorous background check. Efforts are also underway to evaluate the need for improvements to the risk-based approach for background checks for drivers transporting certain types of HAZMAT.

  As employee and "insider" vetting programs proliferate throughout the transportation industry, the DHS, DOT, and the stakeholder community have recognized the inefficiency and potential security gaps that can be created by disparate programs that are not coordinated in purpose or distribution. Because of this concern, the DHS is intensifying its efforts to harmonize vetting programs, background checks, and disqualification standards across modes and purposes.

  The DHS is also working on the Transportation Worker Identification Credential (TWIC) program and will be able to harmonize background check programs. TWIC will focus on those individuals requiring unescorted access to secure areas of Maritime Transportation Security Act (MTSA)-regulated facilities, vessels, and outer continental shelf (OCS) facilities. Under the TWIC program, drivers who have already successfully undergone a security threat assessment to obtain a Hazardous Materials Endorsement (HME) will not be required to obtain a new security threat assessment and will receive a TWIC card for a discounted fee.
- **Security Plans and Training.** DOT regulations (49 Code of Federal Regulations (CFR) 172), effective September 25, 2003, require shippers and carriers of certain HAZMAT deemed to present a security risk in transportation to develop and implement security plans. All shippers and carriers must also ensure that employee training includes a security awareness component. The security plan must be based on an assessment of possible transportation security risks and appropriate measures to address the assessed risks. Specific measures put into place by the plan may vary commensurate with the level of threat at a

particular time. At a minimum, a security plan must address personnel security, unauthorized access, and en route security. The regulations permit a company to implement a security plan tailored to its specific circumstances and operations. DOT modal administrations—such as FMCSA—review security plans as part of ongoing HME programs. Although regulations do not require motor carriers to obtain government approval of security plans, enforcement personnel take advantage of scheduled safety inspections (which include determining whether companies have a security plan) to review security plans and provide informal suggestions for improvement. DOT is evaluating security plan regulations. It is evaluating an industry petition that certain HAZMAT that pose little or no security risk be removed from the list requiring security plans. Other possible changes or clarifications include designating a high-level corporate focal point for HAZMAT security plans, specifying that security plans must be site-based rather than corporate-wide, and adding coverage on government access and review.

Enhance information and intelligence sharing among highway Transportation Systems Sector partners. The development and maintenance of relationships and improved technology can provide Federal, State, local, tribal, private sector, and international transportation security partners with a platform to share and exchange security information such as threats, best practices, lessons learned, or other experiences to improve transportation security.

- **FHWA Security and Emergency Management Professional Capacity Building Program.** FHWA, in partnership with the American Association of State Highway and Transportation Officials (AASHTO), has developed a strategic plan for the security training of State and local transportation officials. This strategic plan for professional capacity building is designed to provide State DOTs with trusted, reliable, and reasonably comprehensive sources of information and assistance to meet their obligations for securing the Nation's transportation network and meeting their emergency response needs. Highlights of the program initiated in fiscal year (FY) 2006 included a pooled-fund solicitation inviting States to contribute funds to support the development and delivery of training, technical assistance and peer support for risk assessment principles and methods, emergency transportation operation, and evacuation planning. In addition, FHWA and TSA initiated a series of regional workshops that brought together security and emergency transportation operations specialists from all States to share best practices and ideas to meet their operational needs.

Goal 2: Enhance the resilience of the U.S. transportation system.

Objectives

Manage and reduce the risk associated with key nodes, links, and flows within critical transportation systems to improve overall network survivability.

- **Integrate Security Measures Into the Design of the Nation's Transportation Network.** Improved methods for cost-effective access control and surveillance/detection will decrease the risk of attack. Design/analysis methods and materials for highway structural hardening, improved standoff distance and barrier designs, and enhanced response/recovery will aid in mitigating risk. Because of the complexity of interacting modes, comprehensive analyses, innovative integrated measures, and tailored training, specialized technology will be required to support intermodal facilities. FHWA currently has a number of programs and resources available to assist highway infrastructure stakeholders recognize and incorporate security measures into the design and construction of highways, bridges, and tunnels.
- **FHWA-Supported Security R&D Program.** FHWA has dedicated a portion of its structural research and development (R&D) program to developing new techniques for enhancing the security and resiliency of highway-related structures. In 2006, FHWA published a report, entitled Multiyear Plan for Bridge and Tunnel Security Research, Development, and Deployment (Report No. FHWA-HRT-06-072), which can be accessed on the Web at www.tfhrc.gov/structur/pubs/06072/index.htm. It presents a strategic plan to secure the Nation's highway infrastructure and is based on input from experts in bridge engineering and other stakeholders. FHWA and the DHS's Science and Technology Directorate are exploring a cooperative relationship in delivering research based on this strategic plan. FHWA is also continuing its cooperative research with the U.S. Army Corps of Engineers (USACE) to develop options for retrofitting existing bridges. Promising advances have been made to pro-

tect some of the Nation's most critical bridge components from terrorist threats through this FHWA-led pooled-fund study. End products will include retrofit options and design guidance on blast-resistant bridge elements for AASHTO consideration.

- **Explore the Use of Existing Grant Programs to Support Critical Highway Infrastructure Security Improvements.** Investments in hardening highway infrastructure can improve highway safety and security. Financial resources to support highway infrastructure hardening are limited, however, and resource decisions can be challenging. The Federal Government will work with State, local, and tribal governments to coordinate specific grants programs with other related grant programs to leverage the benefits from limited resources.

Enhance the capacity for rapid and flexible response and recovery to all-hazards events.

- **FMCSA Hazardous Materials Safety Permit Program.** This program was established on January 1, 2005. Congress directed FMCSA to implement the HAZMAT permit program to produce a safe and secure environment in which to transport certain types of HAZMAT. Within this program lies a requirement for certain motor carriers to maintain a security program and establish a system of communications to enable commercial motor vehicle drivers to contact motor carriers during the course of transportation of these HAZMAT. This safety and security program uses the SCR program to collect specific security information on the motor carrier's ability to secure certain type of HAZMAT.

Goal 3: Improve the cost-effective use of resources for transportation security.

Objectives

Ensure robust sector participation in the development and implementation of public sector programs for the U.S. highway transportation sector.

- **Highway Infrastructure and Motor Carrier GCC and SCC.** The Federal Government uses the Highway GCC and SCC for partnership efforts that provide consensus recommendations regarding security standards and processes. The Federal Government will continue to maintain these partnerships to ensure robust participation from relevant partners in highway transportation sector security.

- **Trucking Security Program (TSP).** This grant program is to sustain the Highway Watch® program to enhance homeland security through increased vigilance and awareness on our Nation's highways. The FY 2006 TSP awarded $4,801,500 (out of a total appropriation of $5 million) directly to ATA. TSP seeks to assist all professionals and operating entities throughout the entire Highway Transportation System in obtaining training on security awareness, reporting suspicious incidents, and information analysis.

- **Infrastructure Protection Program: Intercity Bus Security Grant Program (IBSGP).** The mission of the IBSGP is to, through the distribution of grant money to eligible stakeholders, create 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. The FY 2006 IBSGP awarded $9.5 million. TSA is providing subject matter expertise for evaluating grant applications.

Ensure coordination and enhance risk-base prioritization of research, development, testing, and evaluation efforts.

- **Research the Viable Use of Current and Emerging Security Technologies.** The Federal Government will continue to review the potential use of technology standards for commercial vehicles carrying high-risk cargoes (e.g., toxic inhalation hazards (TIHs), explosives). A recent DOT study showed that some technologies are dual-use, providing improved security benefits, safety benefits, and business efficiencies. These technologies include electronic tracking, panic alerts, driver identification systems, and satellite-based mobile communications tracking. Significant additional R&D on these systems is necessary to demonstrate their effectiveness and inherent security benefits before any reliable strategy and policy can be developed.

3.1.3 Public-Private Partnership Programs

As the owners and operators of transportation assets, the private sector has made contributions toward achieving the goals of the Transportation Systems Sector. Private industry has adopted various security measures that supplement government-led regulations and programs. Industry practices and guidelines focus on achieving security through countermeasures associated with employees/people, information, technology, and physical/cyber infrastructure.

The following three programs are partnerships between private industry and the public sector designed to continually enhance the risk posture of the U.S. highway transportation sector:

- **Intercity Bus Security Grant Program**
- **Truck Security Grant Program**
- **National Cooperative Highway Research Program (NCHRP) Project 20-59.** AASHTO, through its Special Committee on Transportation Security, directs a security and emergency operations R&D program funded through NCHRP, administered by the Transportation Research Board of the National Academy of Sciences. Funding for NCHRP efforts is made available each year from the Federal-Aid Highway Program and is allocated to the various R&D efforts based on problem statements submitted by State DOTs and FHWA. NCHRP Project 20-59 has funded the development of a risk management guide, an emergency transportation operations guide, a guide on managing sensitive information, guidance on continuity-of-operations planning, as well as a number of other more focused reports on topics of special interest. More detailed information can be found at www4.trb.crp.nsf/All+Projects/NCHRP+20-59. The AASHTO Subcommittee on Bridges and Structures also has a committee on bridge security, which provides guidance and support on research needs and for developing research problem statements for implementation through the regular NCHRP program. The committee's role is to ensure that relevant research is conducted that will lead to specific development for design and construction of bridges and structures for security. The committee is also developing a strategic research program for the security of bridges and structures.
- **TSA Missouri Pilot Program.** This pilot program is intended to conduct CSRs of trucking and motorcoach companies using State inspectors. It is the result of a partnership between the Commercial Vehicle Safety Alliance (CVSA), Missouri DOT, and TSA. TSA trained 44 Missouri DOT officers to conduct CSRs while they are also conducting safety inspections for FMCSA.

  Through this program, TSA expects to collect additional security data while testing the feasibility of using roadside enforcement officers to examine security issues. It will also assist the highway and motor carrier industries in collecting and assessing best security practices and providing targeted security assistance. The pilot program began in March 2006 and is expected to run until June 30, 2007. TSA will evaluate the results of this program and determine the feasibility and effectiveness of using State inspectors for CSRs.

3.1.4 Other Initiatives and Pilot Programs

Building on these previous efforts, all sector security partners will continue working together to develop an overarching portfolio of risk-based security programs and countermeasures to improve the highway transportation sector's risk profile and achieve the mode's goals and objectives. The following describes current initiatives and pilot programs:

- **TSA HAZMAT Driver Security Threat Assessments.** Section 1012 of the USA PATRIOT Act of 2001 requires all commercial drivers seeking to apply for, renew, or transfer an HME on their State-issued CDL to undergo a "security threat assessment" to determine whether or not the individual poses a security risk. Individuals may be disqualified from holding an HME based on the assessment, which is comprised of an FBI fingerprint-based criminal history records check, an intelligence check, and immigration status verification. Drivers determined to be a security threat are prevented from receiving HMEs on their CDLs.
- **Truck Tracking Security Pilots.** The ability to track trucks, especially those carrying certain HAZMAT, has potential security benefits. FMCSA has conducted a tracking pilot and TSA is in the midst of conducting one. FMCSA conducted a 2-year

national field operational study of existing technologies offering enhanced solutions to the security of motor carrier shipments of HAZMAT, which was completed in December 2004. The test evaluated the costs, benefits, and operational processes required for wireless communications systems, including global positioning system (GPS) tracking and other technologies. The tested technologies performed well under operational conditions and showed promise for significantly reducing security vulnerabilities. TSA is testing near real-time tracking and identification systems, theft detection and alert systems, motor vehicle disabling systems, and systems to prevent unauthorized operation of trucks and unauthorized access to their cargos. As a result of this pilot, TSA will be able to evaluate such factors as the costs and benefits of the system; the ability to collect, display, and store information on shipments of high-risk materials by motor vehicle and/or trailer throughout the supply chain; and the capability of the system to resist accidental or unauthorized disabling.

- **Hazardous Materials Research Involving Security Initiatives.** The DHS and DOT have current and ongoing R&D projects that will directly impact securing highway transportation facilities, conveyances, and critical infrastructures. Both departments will work closely together to coordinate these projects. FMCSA will be working on congressionally mandated projects and agency-funded projects. One is a continuation of the HAZMAT transportation safety and security testing, including conducting research on the cost-benefit analysis of using truck disabling technologies. FMCSA will also perform testing and evaluation of mobile and stationary radiation detection devices (RDDs) used on trucks. They will also evaluate current routing activities and provide a comprehensive analysis of the safety and security concerns related to HAZMAT routing in the United States. Both departments are also evaluating various commercial software packages designed to assist first-responders when responding to HAZMAT and other transportation incidents.
- **FHWA Statewide and Project-Specific Vulnerability Assessments.** FHWA has trained a cadre of engineers to assess bridges and tunnels for vulnerability to terrorist threats. The engineering assessment team conducts assessments, at the request of the owners, for project-level, facility-level, and statewide critical structures. The objective is to guide facility owners and operators to identify vulnerable components and measures to reduce vulnerability.
- **FHWA Bridge and Tunnel Vulnerability Workshops.** FHWA teamed with USACE to develop training for bridge and tunnel engineers to protect the physical security of critical transportation assets. The workshops address terrorist threats to bridges and tunnels, vulnerabilities to these threats, and potential mitigations to reduce risk.
- **FMCSA Sensitive Security Visit (SSVs) and Security Contact Reviews (SCRs).** FMCSA conducts SSVs and SCRs as part of its regular compliance reviews of HAZMAT carriers. SSVs are educational security discussions covering best practices. They are conducted with HAZMAT motor carriers that do not require a security plan. SCRs are comprehensive reviews of security plans and their implementation that are conducted on all HAZMAT motor carriers that transport placardable amounts of HAZMAT.
- **TSA School Transportation Security Awareness (STSA).** Twenty-five million children ride 500,000 schoolbuses daily in the United States. The TSA Highway and Motor Carrier Division is working with a contractor to develop a school transportation security awareness training program that promotes a better understanding among school transportation personnel of the vulnerabilities of their systems and appropriate mitigation strategies to address those vulnerabilities. The contractor will also create a Facility Security Assessment Program for school entities to use in developing their site-specific security programs. STSA will provide approximately 140 minutes of on-line or on-site training to small groups of personnel in localities that operate schoolbus transportation (schoolbus drivers in particular). The training program will contain significant graphic content and use up-to-date interactive teaching methods. The schoolbus community consists of three major associations: The National School Transportation Association (NSTA), the National Association for Pupil Transportation (NAPT), and the National Association of State Directors of Pupil Transportation Services (NASDPTS). These associations are collaborating with the contractor/vendor, Consolidated Safety Services, Inc., in this security initiative.

- **Evaluation of HAZMAT Security Requirements.** The Federal Government is evaluating the need to harmonize existing security and safety regulations for HAZMAT transport. As appropriate, the Federal Government will solicit and incorporate industry stakeholder input to evaluate; revise; and, where necessary, enhance existing DOT and DHS HAZMAT security regulatory requirements in keeping with current security threats, research, and technologies. Appropriate coordination will be considered for an ongoing effort to evaluate potential subsets of the DOT safety-driven HAZMAT list.

3.1.5 Implementation

The most effective security programs will involve cost-effective security planning, risk assessment, and layered mitigation strategy development. They will also include multi-faceted training and technical assistance to the transportation industry, supported by R&D efforts to promote and advance new security technologies.

TSA, FHWA, and FMCSA are dedicated to improving the security posture of the Nation's highways. All three have developed and implemented initiatives, identified gaps or evaluated vulnerabilities, and are working together and with their industry partners to implement effective mitigation strategies.

3.2 Effective Practices, Security Guidelines, Security Standards, and Compliance and Assessment Processes

Executive Order 13416, Strengthening Surface Transportation Security, requires the identification of existing security guidelines and security requirements for each surface transportation mode. The following describes current regulations and any proposed regulatory actions for highway infrastructure and motor carrier security. The conveyance of HAZMAT poses the greatest threat to the Highway Infrastructure and Motor Carrier Mode. Current regulatory action focuses on mitigation of this threat.

In 2003, DOT established HM-232 (49 CFR 172.800), which requires shippers and carriers of certain highly hazardous materials to develop and implement security plans. In addition, all shippers and carriers of HAZMAT must ensure that their employee training includes a security component.

TSA passed a rule (49 CFR 1570 and 1572) that establishes security threat assessment standards for determining whether an individual poses a security threat warranting denial of an HME for a CDL.TSA will determine that an individual poses a security threat if he or she: (1) is an alien (unless he or she is a lawful permanent resident) or a U.S. citizen who has renounced his or her U.S. citizenship, (2) is wanted or under indictment for certain felonies, (3) has a conviction in a military or civilian court for certain felonies, (4) has been adjudicated as a mental defective or committed to a mental institution, or (5) is considered to pose a security threat based on a review of pertinent databases. The rule establishes conditions under which an individual who has been determined to be a security risk may appeal the determination, and procedures that TSA will follow when considering an appeal. The rule also provides a waiver process for those individuals who otherwise cannot obtain an HME because they have a conviction for a disqualifying felony, or were adjudicated as a mental defective or committed to a mental institution.

Consistent with Executive Order 13416, Strengthening Surface Transportation Security, TSA is drafting SAIs that are voluntary practices designed to improve security for trucks carrying security-sensitive HAZMAT, motorcoaches and schoolbuses, and highway infrastructure. These SAIs are being coordinated with FMCSA and FHWA. Once the SAIs are completed, the Highway SCC will solicit and obtain industry review and input on the SAIs prior to issuance. SAIs, although voluntary, will allow TSA to communicate and share formally with applicable stakeholders those security actions identified as key elements within an effective and layered approach to transportation security. Many of the applicable stakeholders are currently employing some of these security actions as evidenced by the results of highway and motor carrier.

3.3 Grant Programs

Since FY 2003, there have been non-recurring security grant funds for both intercity/charter bus operations and trucks. The security grant money appropriated for trucks supports the ATA's Highway Watch® program, which is described in more detail below. The DHS has administered the distribution of these grant funds.

Figure Annex D3-1: Grant Programs

Program	Program Description	Funding Level FY 2006	Funding Level FY 2007
Intercity Bus Security Grants	See section 3.1, program no. 15	$10 million	$11.64 million
Truck Security Grants	See section 3.1, program no. 16	$5 million	$11.64 million

Intercity Bus Security Grant Program

As a component of the DHS Infrastructure Protection Program (IPP), the IBSGP seeks to assist owners and operators of fixed-route intercity and charter bus services in obtaining the resources required to support the national priorities. Current priorities focus on enhanced planning, passenger and baggage screening programs, facility security enhancements, vehicle and driver protection, as well as training and exercises. The FY 2006 IBSGP directly addresses the DHS National Response Plan and targeted capabilities priorities:

- Expanded regional collaboration;
- Implementation of the National Incident Management System and the National Response Plan;
- Implementation of the interim NIPP;
- Strengthened information-sharing and collaboration capabilities;
- Strengthened interoperable communications; and
- Enhanced chemical, biological, radiological, nuclear, and explosive (CBRNE) detection and response capabilities.

Figure Annex D3-2: Program and Goals/Objectives Matrix

The chart shows the relationship of each project to the Transportation Systems Sector goals and objectives.		Transportation Systems Sector Goals and Objectives												
		Goal 1: Prevent and deter acts of terrorism using or against the U.S. transportation system.	Goal 1A: Implement flexible, layered, and unpredictable security programs using risk management principles.	Goal 1B: Increase the vigilance of travelers and transportation workers.	Goal 1C: Enhance information and intelligence sharing among transportation security partners.	Goal 2: Enhance the resiliency of the U.S. transportation system.	Goal 2A: Manage and reduce the risk associated with key nodes, links, and flows within critical transportation systems to improve overall network survivability.	Goal 2B: Ensure the capacity for rapid and flexible response and recovery to all-hazards events.	Goal 2C: Implement risk-based measures to improve the redundancy and robustness of key nodes, links, and flows.	Goal 3: Improve the cost-effective use of resources for transportation security.	Goal 3A: Align sector resources with the highest priority transportation security risks using both risk and economic analyses as decision criteria.	Goal 3B: Ensure robust sector participation as a partner in developing and implementing public sector programs for CI/KR protection.	Goal 3C: Improve coordination and risk-based prioritization of Transportation Systems Sector security research, development, test, and evaluation efforts.	Goal 3D: Align risk analysis methodologies with the Risk Analysis and Management for Critical Asset Protection (RAMCAP) criteria outlined in the NIPP.
Highway and Motor Carrier Programs	1. FHWA Bridge and Tunnel Vulnerability Workshops		✓	✓			✓	✓	✓					
	2. FHWA Statewide and Project-Specific Vulnerability Assessments		✓	✓			✓	✓	✓		✓			
	3. TSA Security Action Items (SAIs)		✓	✓	✓		✓	✓	✓		✓	✓	✓	
	4. TSA Intercity Bus Security Grant Program (IBSGP)										✓			
	5. TSA Truck Security Grant Program		✓	✓							✓			
	6. FHWA-Supported Security R&D Program		✓				✓							

	The chart shows the relationship of each project to the Transportation Systems Sector goals and objectives.	Transportation Systems Sector Goals and Objectives												
		Goal 1: Prevent and deter acts of terrorism using or against the U.S. transportation system.	Goal 1A: Implement flexible, layered, and unpredictable security programs using risk management principles.	Goal 1B: Increase the vigilance of travelers and transportation workers.	Goal 1C: Enhance information and intelligence sharing among transportation security partners.	Goal 2: Enhance the resiliency of the U.S. transportation system.	Goal 2A: Manage and reduce the risk associated with key nodes, links, and flows within critical transportation systems to improve overall network survivability.	Goal 2B: Ensure the capacity for rapid and flexible response and recovery to all-hazards events.	Goal 2C: Implement risk-based measures to improve the redundancy and robustness of key nodes, links, and flows.	Goal 3: Improve the cost-effective use of resources for transportation security.	Goal 3A: Align sector resources with the highest priority transportation security risks using both risk and economic analyses as decision criteria.	Goal 3B: Ensure robust sector participation as a partner in developing and implementing public sector programs for CI/KR protection.	Goal 3C: Improve coordination and risk-based prioritization of Transportation Systems Sector security research, development, test, and evaluation efforts.	Goal 3D: Align risk analysis methodologies with the Risk Analysis and Management for Critical Asset Protection (RAMCAP) criteria outlined in the NIPP.
Highway and Motor Carrier Programs	7. National Cooperative Highway Research Program Project 20-59		✓				✓					✓		✓
	8. FMCSA and TSA Truck Tracking Security Pilots		✓				✓				✓		✓	
	9. Hazardous Materials Research Involving Security Initiatives		✓								✓			
	10. TSA HAZMAT Driver Background Rulemaking		✓											
	11. FMCSA Hazardous Materials Safety Permit Program		✓				✓							
	12. Security Plans and Training		✓	✓			✓							
	13. FHWA Security Self-Assessment Tool		✓				✓	✓			✓			
	14. TSA Corporate Security Reviews (CSRs)			✓							✓			

	The chart shows the relationship of each project to the Transportation Systems Sector goals and objectives.	Transportation Systems Sector Goals and Objectives												
		Goal 1: Prevent and deter acts of terrorism using or against the U.S. transportation system.	Goal 1A: Implement flexible, layered, and unpredictable security programs using risk management principles.	Goal 1B: Increase the vigilance of travelers and transportation workers.	Goal 1C: Enhance information and intelligence sharing among transportation security partners.	Goal 2: Enhance the resiliency of the U.S. transportation system.	Goal 2A: Manage and reduce the risk associated with key nodes, links, and flows within critical transportation systems to improve overall network survivability.	Goal 2B: Ensure the capacity for rapid and flexible response and recovery to all-hazards events.	Goal 2C: Implement risk-based measures to improve the redundancy and robustness of key nodes, links, and flows.	Goal 3: Improve the cost-effective use of resources for transportation security.	Goal 3A: Align sector resources with the highest priority transportation security risks using both risk and economic analyses as decision criteria.	Goal 3B: Ensure robust sector participation as a partner in developing and implementing public sector programs for CI/KR protection.	Goal 3C: Improve coordination and risk-based prioritization of Transportation Systems Sector security research, development, test, and evaluation efforts.	Goal 3D: Align risk analysis methodologies with the Risk Analysis and Management for Critical Asset Protection (RAMCAP) criteria outlined in the NIPP.
Highway and Motor Carrier Programs	15. TSA Missouri Pilot										✓		✓	
	16. FMCSA Sensitive Security Visits (SSVs) and Security Contact Reviews (SCRs)			✓			✓				✓			
	17. FHWA Security and Emergency Management Professional Capacity Building Program			✓										
	18. TSA School Transportation Security Awareness (STSA)		✓	✓							✓		✓	

In addition, the FY 2006 IBSGP also supports the strengthening of emergency operations planning and citizen protection capabilities, and assistance in addressing security priorities specific to the intercity bus industry. When developing project proposals, specific attention was paid to preventing, detecting, and responding to incidents involving improvised explosive devices (IEDs).

Truck Security

The DHS has also distributed grant money to the commercial motor carrier stakeholder community to improve security awareness and the reporting of suspicious activities. These funds have been directed to the Highway Watch® program, which the ATA administers. With these grant funds, commercial vehicle operators and other highway professionals have implemented domain awareness programs to meet identified security vulnerabilities. These programs include training in awareness and self-protection training for truckers, making significant improvements to first-responder communications, and creating security incident reporting and analysis channels.

3.4 The Way Forward

The Highway GCC will continue to engage the private sector in exploring advances in security and developing programs that are mutually acceptable and will result in increases in security.

There are significant challenges confronting all stakeholders, public and private, directly involved in securing the highway mode of transport. These challenges will have to be overcome before significant and meaningful security improvements can be realized. Before identifying challenges specifically, it is worth mentioning again the complexity and diversity of the Highway Infrastructure and Motor Carrier Mode. It is vast and involves literally tens of thousands of public and private stakeholders. Key components of the Highway Infrastructure and Motor Carrier Mode include: (1) trucking; (2) motorcoaches, charter buses, and schoolbuses; and (3) highway infrastructure, specifically highways, bridges, and tunnels. The first two represent roughly 60,000 stakeholders, mostly trucking and charter bus operators. Secretary of Homeland Security Michael Chertoff frequently reminds the American public "… that while no government can protect every person against every threat in every place at every moment …," the DHS has made and continues to make significant progress to prevent another catastrophic attack against our Nation.

A continuing challenge will be aligning resources and responsibilities. At the Federal level, the key agencies that have a security focus are TSA, FMCSA, FHWA, the Pipeline and Hazardous Material Safety Administration (PHMSA), and the FBI's National Joint Terrorism Task Force (NJTTF). Each agency will need to administratively balance operational needs and requirements to ensure that they meet the commitments of the NIPP and the Transportation Systems SSP. State and local governments will have similar challenges. Additionally, private operators continually try to balance operational demands and costs, and maintain an effective level of security. We must ensure, through a risk-based approach, the maximization of the security effectiveness of the resources available.

Another challenge is synchronizing the Federal approach to establishing regulations, security guidelines, and/or requirements for the Highway Infrastructure and Motor Carrier Mode. Currently, certain DOT agencies, specifically PHMSA and FMCSA, have issued security rules addressing the transportation of HAZMAT and the requirement for security plans. TSA, as stated above in section 3.2, is in the process of developing voluntary security guidelines known as SAIs. These guidelines, prior to distribution, will be developed in concert with DOT and other Federal and industry stakeholders. The coordination process with Federal, State, local, tribal, and private stakeholders should become more routine and streamlined as all become comfortable utilizing the GCC/SCC framework addressed earlier in this plan. This coordination will be very important for ensuring that the issuance of future guidelines, standards, and any other requirements is done effectively and systematically.

Related to the challenge of coordinating the issuance of guidelines, requirements, standards, and regulations is the need to ensure compliance. The challenge of compliance is directly related to the diversity and sheer number of stakeholders men-

tioned in the first paragraph of this section. The effectiveness of any requirement is only as good as the ability to periodically and systematically ensure that all issued requirements have been implemented and are being followed. It will take creative leveraging of resources to develop and implement an effective compliance program.

One of the key security threats in the Highway Infrastructure and Motor Carrier Mode is the potential deliberate misuse of HAZMAT transported on the highway, especially HAZMAT deemed to be particularly dangerous and attractive to terrorists. One of the priorities identified in this plan is to continue to evaluate existing HAZMAT security requirements. The need for the following actions will be further evaluated:

HAZMAT Tracking

Upon completion of the TSA truck tracking pilot in December 2007, further evaluations will be made with regard to requiring that trucks transporting some HAZMAT, such as explosives, TIH, and radioactive materials, be equipped with satellite or terrestrial tracking transceivers enhanced with GPS and be monitored while in transit by a centralized government tracking site. This could provide many benefits: (1) near real-time receipt by the tracking site of emergency alerts generated by trucks; (2) near-immediate tracking site notification to police that an emergency alert has been received; (3) automated identification of in-transit truck delays by the tracking site; (4) the ability of the tracking site to quickly identify and work with industry to divert trucks that are moving toward geographic areas with increased security threat levels; and (5) the ability of TSA to quickly obtain shipment movement records data archived by the tracking site for analysis of the type of shipments moving, when, where, in what quantity, and via what routes. The latter could be a valuable tool for use in conducting analysis to support optimum allocation of scarce security resources. This would constitute a logically progressive use of the tracking technology already in use for the most part by motor carriers transporting the type of HAZMAT noted above.

HAZMAT Shipment Movements to Destination

One of the key means for ensuring the secure movement of some HAZMAT shipments, such as explosives, TIH, and radioactive materials, is to minimize the time in transit and the resultant public exposure. A specific requirement to this end may be considered for these types of shipments. If implemented, this would also have the effect of minimizing the current perceived need for secure and safe areas in which trucks transporting these types of HAZMAT would be able to temporarily stop while in transit. The current practice of permitting stops may actually present more of a security risk due to public knowledge of the sites, and the aggregation of HAZMAT most susceptible to being weaponized by hostile elements.

HAZMAT Shipments Avoiding Standard Routes When Transiting Identified Target Areas

Consideration could be given to requiring that some shipments of HAZMAT, such as explosives, TIH, and radioactive materials, avoid using standard routes when transiting areas identified as target areas for hostile elements. This could maximize unpredictability and thereby increase the difficulty for those elements to conduct attack planning. In order to meet this requirement, some shipments might have to travel a longer distance through areas with potentially smaller roads and less experienced emergency response personnel. This could present a higher risk of an accident. However, the potential increase in safety may be deemed acceptable to mitigate the security risk.

3.5 Metrics

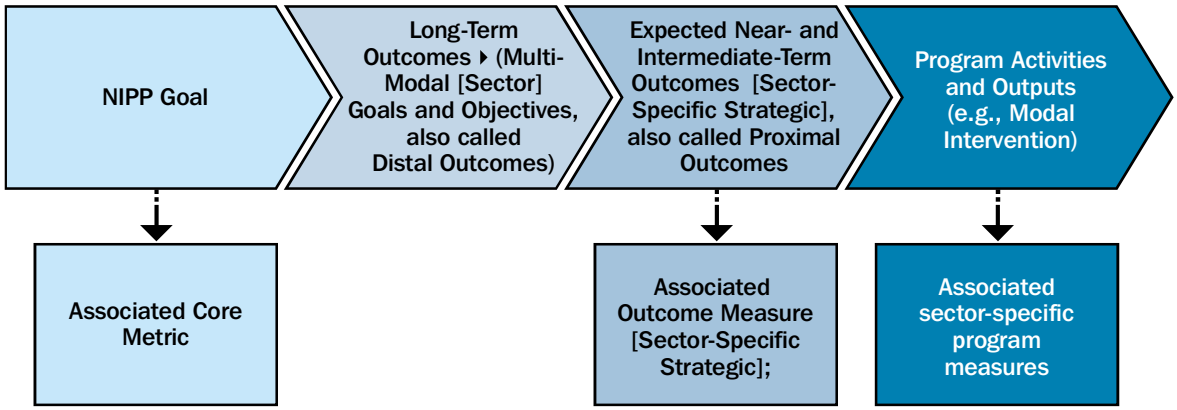
General. To evaluate the collective impact of the Transportation Systems Sector's efforts to mitigate the risks to the transportation infrastructure and to increase the resilience of the transportation system through information-sharing mechanisms, measures of effectiveness will be developed and monitored. Metrics that are developed will supply the data either to affirm that Transportation Systems SSP goals are being met or to show what corrective actions are required. This section is an overview of the plan to implement a Transportation Systems SSP measurement program. To be effective, the measurement program will

require the cooperation of all modal GCCs and SCCs in providing accurate responses to the metrics being used to measure sector risk posture, SSP effectiveness in the sector, and security program effectiveness.

Measurement Joint Working Group. A Measurement Joint Working Group will be formed under the Transportation Systems Sector GCC/SCC and will be comprised of one member from each modal GCC and SCC or their designate and invited measurement professionals. Under the leadership of TSA's lead measurement organization, the working group will operationalize measures; establish data sources, data collection, and verification procedures; set measurement policy for the Transportation Systems SSP; and approve supporting procedures. This entity may also require standardization of certain measurement practices from data contributors across the sector. The Measurement Joint Working Group will communicate regularly with Transportation Systems Sector GCC/SCC members to ensure that working group progress and plans are fully transparent and coordinated with the members. In addition, work products of the Measurement Joint Working Group will be submitted, when appropriate, to the overarching Transportation Systems Sector GCC/SCC for approval.

Measures. The Outcome Monitoring methodology as exemplified in figure 3, Outcome Model, demonstrates working down from the national and multi-modal (sector) goals to determine outcomes and their respective measures.

Figure Annex D3-3: Outcome Model



The Transportation Systems Sector's metrics have been segmented into two categories:

1. **Core:** As discussed in section 6 of the Transportation Systems SSP, core NIPP metrics are common across all sectors and focus on measuring risk-reduction progress in the sector. These measures are often descriptive statistics (counts).
2. **Sector-Specific:** Enhanced Security Measures for Highly Hazardous Materials: There is no statutory mandate to identify high-risk HAZMAT or to require enhanced security measures. TSA is taking a risk-based approach to identifying high-risk substances and working with industry and government stakeholders to develop voluntary measures to reduce the risk. TSA is developing a risk-based approach for targeting CSRs and will increase the number of CSRs conducted from two per month.

3.6 Transportation Systems Sector Goals and Objectives

Goal 1: Prevent and deter acts of terrorism using or against the U.S. transportation system.

1A: Implement flexible, layered, and unpredictable security programs using risk management principles (supported by section 4.1, program nos. 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, and 18).

1B: Increase the vigilance of travelers and transportation workers (supported by section 4.1, program nos. 1, 2, 3, 4, 5, 6, 7, 8, 12, 14, 16, 17, and 18).

1C: Enhance information and intelligence sharing among transportation security partners (supported by section 4.1, program no. 3).

Goal 2: Enhance the resiliency of the U.S. transportation system.

2A: Manage and reduce the risks associated with key nodes, links, and flows within critical transportation systems to improve overall network survivability (supported by section 4.1, program nos. 1, 2, 3, 11, 12, 13, and 16).

2B: Ensure the capacity for rapid and flexible response and recovery to all-hazards events (supported by section 4.1, program nos. 1, 2, 3, and 13).

2C: Implement risk-based measures to improve the redundancy and robustness of key nodes, links, and flows (supported by section 4.1, program nos. 1, 2, and 3).

Goal 3: Improve the cost-effective use of resources for transportation security.

3A: Align sector resources with the highest priority transportation security risks using both risk and economic analyses as decision criteria (supported by section 4.1, program nos. 2, 3, 4, 5, 8, 9, 13, 14, 15, 16, and 18).

3B: Ensure robust sector participation as a partner in the development and implementation of public sector programs for CI/KR protection (supported by section 4.1, program nos. 3 and 7).

3C: Improve coordination and risk-based prioritization of the Transportation Systems Sector security research, development, test, and evaluation efforts (supported by section 4.1, program nos. 3, 8, 15, and 18).

3D: Align risk analysis methodologies with the Risk Analysis and Management for Critical Asset Protection (RAMCAP) criteria outlined in the NIPP (supported by section 4.1, program no. 7).

4 Program Management

The Highway GCC, via a GCC subgroup, will facilitate the coordination and periodic update of this modal implementation plan. Subgroup meetings will be held with interested members of the GCC. In addition, the GCC will coordinate review and updates to this plan with the SCC. Once every year, the GCC and SCC will submit revisions for the Highway Infrastructure and Motor Carrier Modal Annex. Every 3 years, the GCC and SCC will do a complete rewrite of the annex and will update the annex as required or necessary.

5 Security Gaps

Security Plans

Security plans throughout the highway stakeholder community are insufficient. There are few voluntary standards or guidance that reduce vulnerabilities and enhance overall security. TSA is drafting SAIs that are voluntary practices designed to improve security. By developing and distributing these voluntary standards to highway transportation industry partners, they will be able to mitigate security gaps in the following categories: plans, policies, and procedures; training; access control; physical security assets; security technology and equipment; communications security; and information security.

Commercial Driver's License (CDL) Driver Security Threat Assessments

Although assessments are required for drivers applying for or renewing a Hazardous Materials Endorsement (HME) on their CDL, CDL holders do not undergo a security background check as part of the licensing process. Background checks on all CDL holders could reduce the likelihood that a potential security risk would have legal access to trucks and cargo in order to carry out a terrorist or otherwise harmful act. Large vehicles could be used as vehicle-borne improvised explosive devices (VBIEDs) against critical targets, such as was done in Oklahoma City in 1995 and in the 1993 attack against the World Trade Center. Additionally, the lack of secure CDL oversight provided to the agricultural industry by the so-called "farm exemption" in motor carrier regulations leaves a gap in HAZMAT and security regulation coverage. Farm vehicles are capable of transporting dangerous chemicals that could be used to make explosives, such as ammonium nitrate and other HAZMAT.

HAZMAT Carriers

DOT's HM-232 (49 CFR 172.800) requires shippers and carriers of certain highly hazardous materials to develop and implement security plans. However, there are still security gaps that exist in the protection of HAZMAT on the Nation's highways. HAZMAT carrier security gaps include inadequate plans, policies, and procedures; inadequate training; inadequate access controls; inadequate physical security assets; and insufficient security technology and equipment. R&D projects would assist in closing these gaps by providing enhancements in the protection of facilities, conveyances, and critical infrastructure. Implementing technology and security initiatives would also reduce the existing vulnerabilities with regard to the transport of HAZMAT. The Federal Government will continue to review the potential use of technology standards for commercial vehicles carrying high-risk cargoes.

Security Training and Awareness

There is a lack of security-related domain awareness in the areas of CDL schools, motorcoach and commercial truck industries, and schoolbus organizations. Programs to address this gap include Highway Watch, School Bus Watch, School Transportation Security Awareness, Federal Law Enforcement Training Center (FLETC) Roadside Law Enforcement Transportation Security Awareness, and the HAZMAT Motor Carrier Security Self-Assessment Training Project. However, such programs do not cover the entire spectrum of highway transportation. More comprehensive security training and awareness programs would ensure that highway transportation and law enforcement personnel are better prepared to address these gaps.

Schoolbus Security Training

There is a lack of sufficient security training for the schoolbus industry in the United States. Although there are more than 500,000 schoolbus employees, there are extremely limited numbers of security training curriculums designed specifically for this critical transportation community. Additional and more comprehensive training is needed to cover this large population. The lack of training and security awareness is a substantial gap that, when addressed, would greatly enhance security for operators, passengers, and the public in general. TSA is beginning to address this training gap with support for two programs: the School Transportation Security Awareness program, and the School Bus Watch program (a grant-funded program run by the American Trucking Associations). However, an increased focus on the areas of prevention and protection training, communication strategies, and response and recovery training would do the most to reduce this gap.

Annex E. Freight Rail

1 Executive Summary

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. While there are no specific threat or intelligence points to freight rail transportation, the potential exists for using the freight rail system as a target for terrorism or as a delivery system for a weapon of mass effect.

The efficient operation of our critical interstate freight rail network requires a uniform nationwide approach to railroad security. The Department of Homeland Security (DHS) will continue to work with its private sector, and Federal, State, and local partners to achieve the Transportation Systems Sector goals outlined in this document.

The freight rail mode will continue to apply the National Infrastructure Protection Plan (NIPP) risk management framework for developing programs and initiatives to enhance the protection of critical infrastructure and key resources (CI/KR). As outlined in section 1 of the Transportation Systems Sector-Specific Plan (SSP), the Transportation Systems Sector identified three goals to help achieve the sector vision of a "secure, resilient, and efficient transportation network." The freight rail mode will focus on these goals when identifying key assets and will evaluate consequence, vulnerability, and threat information to adequately assess the risks facing the system. Initial security gaps have been identified, and security programs have been developed and implemented to mitigate these risks. The government continuously evaluates security gaps in freight rail, as in all modes. Mitigation strategies are updated as gaps are identified.

The freight rail mode supports the Transportation Systems SSP goals and objectives through these tools: (1) high-threat urban area (HTUA) rail corridor assessments and comprehensive reviews, (2) inspections/implementation surveys, and (3) industry reporting of baseline data. These tools provide the government with sufficient domain awareness to determine programmatic priorities. As outlined in the NIPP, emphasis will be placed on continuous improvement to enhance protection of freight rail CI/KR.

2 Overview of Mode

2.1 Vision of Mode

The freight rail mode's vision is to protect the Nation's freight rail network from terrorist or criminal attacks and prevent terrorists or other criminals from using freight rail conveyances and their cargoes as weapons of mass effect to attack the public or critical infrastructure.

2.2 Description of Mode

Since the early 19th century, freight railroads have been a principal carrier for moving freight in the United States. U.S. freight railroads are the world's busiest, moving more freight than any other rail system in the world. U.S. railroads operate more than 140,000 miles of track and earn $42 billion in annual revenues. U.S. railroads are vital to our economy, national defense, and public health. Forty percent of all intercity freight goes by rail, including 64 percent of the coal used by electric utilities.

As of 2004, there were 558 common carrier freight railroads operating in the United States. Railroads are classed based on operating revenue. Class I137 railroads have revenues of at least $289.4 million. Seven railroads met this benchmark in 2004. Class I carriers comprise just 1 percent of freight railroads, but account for 70 percent of the industry's mileage operated, 89 percent of its employees, and 93 percent of its freight revenue. Class I railroads operate in many different States and largely concentrate, though not exclusively, on long-haul, high-density intercity traffic lines.

The remaining 551 railroads are divided into two groups—the short line and regional railroads. Regional railroads are defined as operating at least 350 miles of railroad and earning between $23.1 million and $289.3 million annually in operating revenues. The short line railroads traditionally have even lower mileage and revenues below $23.1 million. Short line railroads can be further divided into local line-haul railroads and switching/terminal railroads. Switching and terminal carriers perform primarily switch service or terminal service, as applicable, in cities that are served by more than one carrier. Terminal railroads are often owned by one or more of the Class I[62] railroads. In most major metropolitan areas, a loss of service from the belt railroad, a type of short line, or terminal railroad would severely hamper interchange operations between eastern and western rail Class I carriers.

Railroads provide critical support to the Department of Defense (DoD) Strategic Rail Corridor Network (STRACNET), which includes more than 30,000 miles of rail line and provides the backbone for transporting DoD shipments.

Freight railroads concentrate on hauling bulk commodities and large-quantity shipments over long distances. Based on volume, railroads transport 12.7 percent of the Nation's goods. Most railroad revenue and tonnage comes from hauling coal, chemicals and allied products, non-metal minerals, food and kindred products, and transportation equipment (automobiles). Most of the commodities present little or no target value for terrorists. However, as accidents such as the January 2005 Graniteville, SC, train derailment demonstrated, the release of toxic inhalation hazard (TIH) materials (e.g., chlorine, ammonia, and sulfur dioxide) can cause devastating and lethal consequences. In South Carolina, the ruptured tank car carrying chlorine caused 9 deaths, treatment of 75 people for chlorine exposure, and the evacuation of more than 5,400 people within a 1-mile radius for several days. Likewise, a deliberate terrorist attack against TIH materials in transportation poses serious risks of fatalities and injuries.

According to the Department of Transportation's (DOT's) Bureau of Transportation Statistics, hazardous materials (HAZMAT) traverse more than 72 trillion ton-miles on rail. HAZMAT are essential to the functioning of the economy and society. They fuel motor vehicles, purify drinking water, and heat and cool homes and offices. Other HAZMAT are used for farming and medical applications, and for manufacturing, mining, and other industrial processes.

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 transfers from the maritime mode to freight rail are international movements. These shipments have either a North American destination or a European destination. The use of the continental United States by foreign shippers and consignees as a "land bridge" is a practice that is continuing to grow.

[137] Five of the Class I railroads are U.S.-owned: (1) BNSF Railway (BNSF), (2) CSX Transportation (CSX), (3) Union Pacific (UP), (4) Kansas City Southern (KCS), and (5) Norfolk Southern (NS); two are owned by Canadian companies: (1) Canadian Pacific (CP), and (2) Canadian National (CN).

In addition to being part of the overall cargo system, the freight rail system has its own closed intercarrier system whereby carriers transfer cars to and from one another to efficiently transport goods across the United States. This system is facilitated by interchange agreements, joint services, and voluntary access agreements that allow a carrier to operate over the tracks of another railroad. The government's role here is to assist in providing a safe, secure, and cost-effective transportation system for the Nation, while preserving competition.

Freight Rail Statistics[138]

Class I carriers generate 93 percent of freight revenues and employ 89 percent of railroad workers

- 1.6 million HAZMAT originations in the United States and Canada annually
- 1.2 million tank car originations annually
- Liquefied Petroleum Gas (LPG): 85,198 tank car shipments (2003)
- Chlorine: 30,254 tank car shipments (2003)
- Anhydrous ammonia: 30,687 tank car shipments (2003)
- Food and agricultural commodities: 407 million tons (2003)
- Miles of railroad operated: More than 140,000 miles
- Freight cars in service: 642,405
- Locomotives in service: 22,548

2.3 Government Coordinating Council/Sector Coordinating Council Structure and Process

As outlined in the Freight Rail Government Coordinating Council's (GCC) charter, the objective of the Freight Rail GCC is to coordinate security strategies and activities; establish policies, and guidelines; and develop program metrics and performance criteria for the freight rail mode. Specifically related to developing the SSP modal implementation plan, the Freight Rail GCC will identify security needs and outline programs, policies, and procedures in the plan and work to address any gaps. The Freight Rail GCC will complete this work by creating working groups to address specific issues. The Freight Rail GCC will meet every 2 months. The Freight Rail GCC will offer to meet with the Freight Rail Sector Coordinating Council (SCC) quarterly to address critical issues, or as necessary as critical issues develop.

The Freight Rail SCC is the industry counterpart to the Freight Rail GCC and was established in mid-2006. The Freight Rail GCC will work with the Freight Rail SCC to build strong partnerships to address the common vision of securing the Freight Rail mode.

GCC Membership

Department of Homeland Security

- Transportation Security Administration (TSA)
- Transportation Sector Network Management
- National Protection and Programs Directorate

[138] The statistics listed come from Association of American Railroads (AAR) Railroad Facts, 2005 edition, and AAR and Bureau of Explosives Annual Report of Hazardous Materials Transported by Rail, July 2005 edition.

- Federal Emergency Management Agency, National Preparedness Directorate
- Office of Grants and Training
- Office of Intergovernmental Programs
- U.S. Coast Guard (USCG)
- Customs and Border Protection (CBP)

Department of Transportation (DOT)

- Federal Railroad Administration (FRA)
- Pipeline and Hazardous Materials Safety Administration (PHMSA)
- Surface Transportation Board

Department of Justice

- Federal Bureau of Investigation (FBI)

Department of Defense

- Assistant Deputy Under Secretary of Defense (Transportation Policy)

SCC Membership

- Association of American Railroads (AAR)
- American Short Line and Regional Railroad Association (ASLRRA)
- 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

3 Implementation Plan

3.1 Goals, Objectives, and Programs/Processes

The Department of Homeland Security (DHS) has outlined three goals for the transportation sector. Each goal is supported by objectives that assist in focusing the mode's programs and initiatives to meet that specific goal.

3.1.1 Freight Rail Mode Goals and Objectives

Goal 1: Prevent and deter acts of terrorism using or against the transportation system.

Most freight rail security programs are currently designed to promote Goal 1. DHS programs are designed to provide the government with maximum domain awareness, thus allowing the best possible risk analysis. A thorough and accurate risk analysis allows us to meet Goal 1 by identifying and mitigating vulnerabilities through layered protective measures.

Objectives

Implement flexible, layered, and effective security programs using risk management principles. The freight rail sector will develop and implement layered security programs using risk management principles (discussed in sections 3 through 7 of the Transportation Systems SSP). The DHS and DOT have programs in place to assess the risk to the freight rail sector at both the system and asset levels:

- **High Threat Urban Area (HTUA) Rail Corridor Assessments.** These assessments focus on assessing the vulnerabilities of high-population areas where TIH materials are moved by rail in significant quantities. Assessments are conducted by teams comprised of subject matter experts from TSA, FRA, PHMSA, DHS, the affected railroads, and State and local homeland security officials. Each assessment may consist of four phases: (1) request for information to the carrier, (2) scoping visit, (3) "Boots on Ground" assessment, and (4) tabletop exercises with the carrier. These assessments aid DHS and DOT in identifying critical control points (areas of high consequence and vulnerability) at each location. The critical control points are reviewed using current threat scenarios, and mitigation strategies are 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. The results of the HTUA assessments supported the development of the Recommended Security Action Items (SAIs) issued by DHS and DOT on June 23, 2006.
- **Comprehensive Reviews.** Comprehensive Reviews are a larger scale, more encompassing version of the HTUA rail corridor assessments. Comprehensive Reviewas 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. Team members include response and recovery officials from all levels of government and DHS personnel in order to gain additional perspective and effectively target security grant dollars.
- **Corporate Security Reviews (CSR).** The CSR program is an "instructive" review of a company's security plan and procedures that provides the government with a general understanding of each freight railroad's ability to protect its critical assets and its methods for protecting HAZMAT under its control. Teams of government experts analyze the railroad's security plan for sufficiency, determine the degree that 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.

Current priorities are based on the asymmetrical threat to the freight rail system, focusing on the consequence calculation. The greatest consequence comes from weaponizing the freight rail conveyance itself by using a loaded TIH[139] railcar as a weapon of mass effect. This would most likely be accomplished by attaching an improvised explosive device (IED) to an unattended, standing TIH car in an HTUA or to a car that would enter an HTUA. A less likely scenario, also using the transportation system as a weapon delivery system, is using an intermodal container to deliver a weapon of mass effect to a major target city. In this scenario, a container is loaded with a weapon of mass effect and shipped to a U.S. destination. The container is carried via the freight rail system to its target.

In coordination with the railroads, TSA, FRA, and PHMSA developed a comprehensive list of performance-based SAIs[140] to foster an enhanced security posture in the freight rail mode in general, and in transporting TIH materials in particular. Based on the findings from the HTUA rail corridor assessments, operational practices that enhance the security of TIH shipments were identified and compiled into a list of SAIs. These practices are recommended and voluntary. They provide a basis for driving standardized security measures throughout the industry and address system security, access control, and en route security. DHS and DOT issued the SAIs to industry on June 23, 2006. Almost all SAIs were developed in concurrence with the railroad industry.

TSA and FRA developed Supplement No. 1 to the SAIs listed above. The Federal Government issued Supplement No. 1 to industry on November 21, 2006. The action items addressed in Supplement No. 1 concern the security of the transportation of TIH in HTUAs and cover four main areas:

- Establishment of secure storage areas for railcars carrying TIH materials;
- Expedited movement of trains transporting railcars carrying TIH materials;
- Positive and secure handoff of TIH railcars at points of carrier interchange and points of origination and delivery; and
- Minimization of unattended, loaded tank cars carrying TIH materials.

These four areas should be addressed in TSA-recommended site-specific security plans.

Built into Supplement No. 1 is a strategy to reduce the risk of transporting bulk TIH through HTUAs. The strategy includes the freight railroads providing TSA with baseline data on unattended, standing, loaded TIH cars. TSA is analyzing this data in order to reduce the risk from TIH in transportation by 50 percent by the end of 2008. As with the original SAIs, Supplement No. 1 is recommended and voluntary.

Increase the vigilance of freight rail workers. The Federal Government places a high premium on security training for frontline personnel. PHMSA requires security awareness training for HAZMAT employees. Training must include recognizing and responding to possible security threats and indepth security training.[141] FRA enforces this provision and measures effectiveness on a regular basis. Additionally, the Federal Government provides voluntary standards through the distribution of professional-quality training packages to rail carriers that supplement existing industry security training programs.

TSA is establishing a series of employee training courses focused on supplementing industry programs. Training will be coordinated with industry security personnel prior to issuance. DHS plans to issue a "train the trainer" video course to train HAZMAT employees who work with railroad cars to look for and identify IEDs attached to railcars, engines, or adjacent equipment. TSA is planning to release other supplementary training material, including a security awareness training package for operational employees and security awareness training for all railroad employees.

[139] TIH are materials that are "so toxic to humans as to pose a hazard to health during transportation." See 49 CFR 173.115 (c)(1) (2005). Examples of TIH include chlorine, anhydrous ammonia, ethylene oxide, and fuming sulfuric acid.
[140] Issued June 23, 2006; and November 21, 2006 and February 12, 2007. These can be found on TSA's Web site, www.tsa.gov. The DHS-designated HTUAs can also be found on the TSA Web site.
[141] 49 CFR 172.704 (a)(4), (5).

Enhance information and intelligence sharing among freight rail security partners. TSA provides industry with threat information daily after a thorough analysis of open-source information. TSA distributes relevant freight rail intelligence to railroad stakeholders. Communications between government and industry are supported through two important programs the GCCs and SCCs, and the Homeland Security Information Network (HSIN).[142]

The Federal Government maintains good intra-governmental relationships and strong government ties with industry. TSA has signed two memorandum of understanding (MOU) annexes with its DOT counterparts. The annex with PHMSA was signed on August 9, 2006. The annex with FRA was signed on September 28, 2006. Each annex addresses communications between agencies.

Mechanisms are in place at the industry level to share information. AAR uses three mechanisms to share information with its membership and the ASLRRA membership: (1) the Surface Transportation Information Sharing and Analysis Center (ISAC), (2) the Railway Alert Network (RAN), and (3) the AAR Security Operations Center Implementation Plan. The AAR Operations Center is the hub of RAN; the Surface Transportation ISAC is linked to the AAR Operations Center and provides physical and cyber threat and warning information. The FBI National Joint Terrorism Task Force Railroad Police Liaison (RPL) reports directly to the seven Class I railroad police chiefs on terrorism and intelligence matters having relevance to rail operations.

Goal 2: Enhance the resiliency of the U.S. transportation system.

The freight railroads have undertaken efforts to enhance the resiliency of the freight rail transportation system. After September 11, 2001, AAR developed a Security Management Plan that serves as both a national plan and a template for developing a railroad's own individual security plan. The AAR plan encompasses the principles of threat assessment and risk assessment to cover the entire railroad industry. It supports Objective 1 of Goal 2 as the plan provides a management strategy to reduce the risk associated with the key nodes, links, and flows of the network. The AAR plan supports Objective 2 in establishing a system to gain quick intelligence and respond quickly to all-hazards events, which enhances the capacity for rapid and flexible response and recovery.

Additionally, the plan outlines countermeasures, derived from a risk assessment of the entire network, that span across all railroad functions. Some of these countermeasures include permanent changes to procedures and operations, such as restricted access to facilities, increased tracking of certain shipments, enhanced employee security training, and cyber security improvements at certain threat levels.

Objectives

Manage and reduce the risk associated with key nodes, links, and flows within critical transportation systems to improve overall network survivability. Freight rail security priorities are determined on the basis of risk. Risk is a function of threat, vulnerability, and consequence. As outlined in section 3 of the Transportation Systems SSP, freight rail policy, like all of transportation policy, is primarily driven by considerations of consequence or measures of loss of life and human injury, economic losses, and restoration costs. The most important freight rail security objective is reducing the risk of TIH cars in transportation. This objective has been further narrowed to minimizing the aggregate number of hours that loaded, unattended TIH cars stand in HTUAs.[143] Additional security objectives will be defined as government and private sector initiatives lower the risk from TIH cars.

The Federal Government implements risk-based measures to improve the redundancy and/or robustness of key nodes, links, and flows through CSRs supplemented with the same programs as Goal 1. The reviews provide a corporate operations snapshot and the ability to identify vulnerabilities or chokepoints in an individual carrier's system. CSRs supplement freight rail programs that are centered on prevention and deterrence, making key nodes more robust. Redundancy is already built into the

[142] See appendix A of the Transportation Systems SSP for further discussion.

[143] DHS chose to use the HTUAs designated by DHS under the Urban Area Security Initiative for 2006 as an initial starting point for focusing resources since these areas have large populations. DHS determined that the conducted risk assessments indicate sufficient risk to warrant awarding the areas Federal security grant dollars. HTUAs that do not support TIH rail traffic, such as San Diego, CA, and Honolulu, HI, are not included in measures that cover TIH rail transportation.

freight rail system; therefore, additional programs focused on resiliency and redundancy must be closely examined to ensure that they are cost-effective in meeting the security goal that they are designed to achieve.

Enhance the capacity for rapid and flexible response and recovery to all-hazards events. The freight rail sector relies on sophisticated planning and practices that supplement local first-responders to quickly recover from an all-hazards event. The railroad industry has a long history of planning for and responding to natural and manmade disasters, and has systems in place to respond and recover quickly to all events. Railroads have contracted with specialist companies for re-railing equipment and responding to and cleaning up HAZMAT spills. Redundancy is already built into the freight rail system; railroads have plans in place, including the use of alternate routes if track or other infrastructure is damaged, to initiate recovery as soon as possible. Railroads have in place mutual help agreements as part of their business continuity plans. For example, one railroad was able to rebuild more than five miles of bridge over Lake Pontchartrain in just 16 days after it was destroyed by Hurricane Katrina in 2005.

Goal 3: Improve the cost-effective use of resources for transportation security.

Objectives

Align sector resources with the highest priority security risks using both risk and economic analyses as decision criteria. By identifying the current baseline level of risk for freight rail transportation, focusing on type of cargo and route, and determining how current and potential programs will lower that baseline risk, the Federal Government will be able to effectively align limited resources with the highest priority security risks. Working through the Freight Rail Transportation, Chemical, and Energy GCCs and SCCs, the economic considerations of the industry are taken into account.

The DHS Office of Infrastructure Protection (IP) issues Protective Measures reports that describe likely terrorist objectives, methods of attack, and corresponding protective measures and their implementation in accordance with the Homeland Security Advisory System (HSAS). IP has determined measures specific for freight rail systems at each level of the HSAS that can be quickly disseminated if the threat requires or in the event of an incident.

Ensure robust sector participation in the development and implementation of public sector programs for freight rail protection. The Federal Government maintains close partnerships with the freight rail industry and with key representatives from the shipping industry. The Federal Government uses the Freight Rail GCC and Freight Rail SCC for partnership efforts and intends to reach out to other SCCs as appropriate. These outreach efforts provide recommendations regarding security standards and processes. When developing mandatory standards, the Federal Government, whenever possible, uses traditional notice and comment rulemaking, allowing the general public to provide valuable feedback on operational feasibility, usefulness of the proposal, and cost.

Ensure coordination and enhanced risk-base prioritization of research, development, testing, and evaluation efforts. The Federal Government is pursuing long-term research efforts aimed at improving the transportation security of HAZMAT by rail. DOT is researching the crashworthiness of HAZMAT tank cars, which may lead to revised safety standards that will probably have residual security benefits. The AAR Tank Car Committee is also considering crashworthiness. DOT, in cooperation with the railroad, tank car, and chemical industries, is conducting research on materials, such as protective coatings that might resist certain forms of attack— specifically, the amounts and impacts of explosives, incendiary devices, and stand-off weapons necessary to breach a rail tank car carrying HAZMAT. Release scenarios, source terms, plume modeling, and risk characterization are being pursued to better understand the consequences of an event. DOT, in coordination with DHS, is testing a cooperative HAZMAT transportation research program with a strong security component to bring together the varied stakeholders in government, industry, and the public to help define and pursue a common research agenda.

3.1.2 Private Sector Programs and Processes

In the aftermath of 9/11, the freight rail industry undertook important security measures to mitigate and address vulnerabilities, largely of its own initiative. The industry initiative produced voluntary guidelines that enhanced security in freight rail transportation and assisted in meeting the security goals and objectives of the sector. The Federal Government will continue to

support the private sector's security investments through its own programs and initiatives, and will continue to engage industry in the SCC process to ensure a comprehensive strategy for freight rail security.

AAR Terrorism Risk Analysis and Security Management Plan

After 9/11, AAR developed a security plan for transporting freight in North America. Given that security at that time was primarily focused on loss prevention, after implementation, the AAR plan raised the security baseline in the United States. The AAR plan served as the first building block for freight rail security for TSA at its creation in 2002. The Federal Government has been building and raising the baseline ever since. The AAR plan can also serve as a template for rail carrier-specific security plans.

The Emergency Response Training Center at the Transportation Technology Center, Inc. (TTCI)

TTCI offers advanced emergency response training at its Colorado facilities and at customer locations worldwide. TTCI is owned by DOT's FRA and operated by Transportation Technology Center, Inc., a for-profit subsidiary of the AAR. The curriculum is based on Occupational Safety and Health Administration, National Fire Protection Association, Federal Emergency Management Agency National Preparedness Directorate, and Department of Transportation requirements.

TIH Shipping Industry Partners

After 9/11, Responsible Care® companies took the lead in quickly adopting the Responsible Care® Security Code, an aggressive facility security program, to further protect chemical facilities, chemical transportation systems, communities, and products. Implementation of the Responsible Care® Security Code is required of all American Chemistry Council (ACC) members and Responsible Care® Partners. Under the Security Code—which addresses facility, cyber, and transportation security—companies conduct comprehensive facility security vulnerability assessments, implement security enhancements, and obtain independent verification of facility enhancements. Implementation of the code requires following a strict timeline and mandatory periodic progress reports. Freight railroads that adhere to the AAR Security Management Plan are deemed compliant with the ACC's Responsible Care® Security Code.

Additionally, the Chlorine Institute (CI) developed the Chlorine Rail Transportation Security Management Plan to assist members and their customers in developing security plans to protect chlorine tank cars. When it became evident that a similar document was needed for all poison inhalation hazard (PIH)[144] tank cars, CI and ACC used the Chlorine Rail Transportation Security Management Plan to develop Responsible Care® Value Chain Implementation Guidance: Transportation of PIH Materials by Rail (ACC/CI PIH plan). This plan is designed to provide guidance for developing a seamless security program between chemical shippers, chemical customers, and the railroads. It is compatible with the AAR Security Management Plan.

Transportation Community Awareness and Emergency Response (TRANSCAER)

TRANSCAER is a voluntary national outreach effort that focuses on assisting communities to prepare for and respond to a possible HAZMAT transportation incident. TRANSCAER members are volunteer representatives from the chemical manufacturing, transportation, distribution, and emergency response industries, as well as the government. Each year, at hundreds of sites nationwide, TRANSCAER provides thousands of emergency responders and local officials with unique, hands-on training using actual transportation equipment.

Railway Alert Network (RAN)

RAN is controlled by the AAR Operations Center, which links Federal national security and military personnel, and major customer associations with the freight railroads on a 24 hours per day, 7 days per week (24/7) basis. The Surface Transportation ISAC, also a 24/7 facility, is also linked to and supports RAN. The freight railroad industry is linked to the law enforcement community through individual railroad police departments and through the National Joint Terrorism Task Force, where a

[144] **PIH and TIH are synonymous.**

railroad police officer resides. The system, as a whole, is used to research, receive, analyze, and transmit security information that supports AAR decisionmaking relative to appropriate AAR alert level actions.

AAR Operations Center

The AAR Operations Center collects, analyzes, and disseminates information on physical threats to railroad operations. It operates RAN, through which AAR declares appropriate AAR freight railroad security alert levels. The Surface Transportation ISAC collects, analyzes, and disseminates information on physical and cyber threats. It is linked to the AAR Operations Center and Surface Transportation ISAC members. The AAR Operations Center operates at, or can operate at, the secure level to address intelligence and information-sharing issues.

3.1.3 Other Initiatives and Pilot Programs

Building on these previous efforts, all sector security partners will continue working together to develop an overarching portfolio of risk-based security programs and countermeasures to improve the freight rail mode's risk profile and achieve the mode's goals and objectives. The following describes current initiatives and pilot programs with the goal that each is intended to support.

Intrusion Detection
Department/Agency: TSA and FRA
Goal: Enhance the resiliency of the U.S. transportation system.

Critical freight rail infrastructure includes railroad tracks, bridges, and tunnels. TSA and FRA are looking at various technologies to identify trespassers on rail bridges and tunnels to deter terrorist intelligence gathering and to prevent the placement of a foreign object into the system. Ground-penetrating radar is being investigated to determine substructure problems along railroad track. Radar could also be used for detecting bombs or other foreign objects introduced into the system.

Security Situational Awareness
Department/Agency: DOT
Goal: Improve the cost-effective use of resources for transportation security.

FRA has funded the John A. Volpe National Transportation Systems Center's concept for a situation display that could inform transportation operators, emergency management officials, and policymakers of key interrelationships and the status of critical systems, particularly transportation systems. The concept evolves from two sources: (1) the application of situation displays to cross-cut transportation problems, and (2) the need for comprehensive tools to address the complexity of homeland security issues. FRA and the National Aeronautics and Space Administration (NASA) currently sponsor the Transportation Security Situation Display (TSSD). TSSD involves a public-private partnership among the Volpe Center, the City of New York Office of Emergency Management, and Silicon Graphics Federal, Inc. TSSD is designed as a multi-use tool that supports situational awareness, command and control operations, planning, simulations, research, training, and re-analysis of past events. Once operational, it is expected to have three-dimensional urban imagery with data visualization, zoom capabilities, and high-spatial resolution.

Railroad Vehicle and Cargo Inspection System (Railroad VACIS®)
Department/Agency: CBP
Goal: Prevent and deter acts of terrorism using or against the transportation system.

Railroad VACIS® is unique; it is the only available method for non-invasive inspection of loaded and moving railroad cars. It uses a proprietary gamma ray imaging technique requiring a very low radiation dose. This technique compares favorably against older techniques using x-rays for large-object inspection. It can be operated without a special protective building or similar enclosure, which increases the system's simplicity and decreases the purchase price. Railroad VACIS® is capable of inspecting trains traveling at speeds of between 1 and 7 miles per hour (mi/h). As the railcars move through the gamma beam, their images are individually saved, along with radio frequency identification (RFID) data and a digital video snapshot

of the car identification (ID) number. The Railroad VACIS® operator can view the images as they are acquired and make the appropriate decisions to further inspect the railcars if necessary.

Tank Car Tracking Project
Department/Agency: TSA and FRA
Goal: Prevent and deter acts of terrorism using or against the transportation system.

TSA is examining alternatives to single-car tracking to determine whether the necessary degree of detail and timeliness can be achieved by using existing railcar location management systems. Currently, most railroads and their customers track the location of the cars using wayside detectors and RFID tags. This system, Automatic Equipment Identification (AEI), provides an historical record of the last reported location and a trip history of railcars and locomotives. TSA has partnered with FRA in a pilot project with Railinc, a private data service provider, to obtain car location reports on an as-requested basis. The project will provide the government with timely car location reports on all TIH and other selected HAZMAT cars. Railinc manages the shipping and car location management data interchange for the Nation's freight railroads. It developed a suite of software called FreightScope™ to assist smaller railroads in managing railcar movement records. Railinc has tailored the FreightScope™ reports to meet the government's safety and security information needs. TSA and FRA will be testing the informational and operational capabilities of the program during a pilot project.

National Capital Region Rail Pilot Project
Department/Agency: DHS
Goal: Enhance the resiliency of the U.S. transportation system.

The National Capital Region Rail Pilot Project (NCRRPP) is an intelligent video-based security program that provides security enhancements along the District of Columbia rail corridor. This program will include two central projects: (1) a virtual fence surrounding the area of concern, and (2) virtual gates at each entry point to NCRRPP. NCRRPP also includes intelligent video surveillance of rail lines through critical areas (as designated by DHS), as well as intruder detection software with the capability of identifying unauthorized personnel. The system architecture will be flexible, allowing DHS to incorporate additional technologies into the project as they become available. These technologies include advanced biological and chemical warfare agent detectors currently in development. The system will provide 24/7 monitoring capability in real-time streaming video and, as directed by DHS, will infuse data and alarm information from the railroad's communications center and from other multiple remote locations.

3.2 Security Guidelines and Security Standards, and Compliance and Assessment Processes

Executive Order 13416 requires the identification of existing security guidelines and security requirements for each surface transportation mode. The following describes current regulations and any proposed regulatory action for freight rail security.

3.2.1 Security Guidelines and Security Standards

DOT Security Plan Regulation, 49 CFR 172.800
Department/Agency: PHMSA and FRA
Goal: Prevent and deter acts of terrorism using or against the transportation system.

DOT requires shippers and carriers of HAZMAT deemed to present a transportation security risk to develop and implement a security plan. The security plan must be based on an assessment of possible transportation security risks. Specific measures may vary commensurate with the threat level. At a minimum, the plan must address personnel security, unauthorized access, and en route security. FRA reviews the security plans as part of its ongoing HAZMAT enforcement program. Government approval of security plans is not required; however, FRA enforcement personnel provide informal suggestions for improvement. DHS and DOT are considering revisions to security plan regulations.

48-Hour Rule, 49 CFR 174.14
Department/Agency: PHMSA and FRA
Goal: Prevent and deter acts of terrorism using or against the transportation system.

DOT requires that each shipment of HAZMAT be forwarded "promptly and within 48 hours (Saturdays, Sundays, and holidays excluded)" after acceptance of the shipment by the railroad carrier.[145] If only biweekly or weekly service is performed, the carrier must forward a shipment of HAZMAT in the first available train. Additionally, carriers are prohibited from holding, subject to forwarding orders, tank cars loaded with Division 2.1 (flammable gas), Division 2.3 (poisonous gas), or Class 3 (flammable liquid) materials. FRA enforces this provision.

Hazardous Materials: Enhancing Rail Transportation Safety and Security for Hazardous Materials Shipments Notice of Proposed Rulemaking (NPRM), published on December 21, 2006, 49 FR 76834
Department/Agency: PHMSA and FRA
Goal: Prevent and deter acts of terrorism using or against the transportation system.

DOT, in consultation with TSA proposed a revision to the current requirements in the Hazardous Materials Regulations that are applicable to the safe and secure transportation of specified HAZMAT transported in commerce by rail. Specifically, DOT proposed requiring that rail carriers compile annual data on specified shipments of HAZMAT. PHMSA proposed that data will be used to analyze safety and security risks along rail transportation routes where specified materials are transported, assess alternative routing options, and make routing decisions based on those assessments. PHMSA also proposed clarification of the current security plan requirements to address en route storage and delays in transit and additional security inspection requirements for HAZMAT shipments.

Rail Security NPRM, published on December 21, 2006, 49 FR 76852
Department/Agency: TSA
Goal: Prevent and deter acts of terrorism using or against the transportation system.

TSA proposed the establishment of security requirements for rail transportation, including certain shippers and receivers of specified categories and quantities of HAZMAT.[146] Specifically, TSA proposed requiring freight railroad carriers and fixed-site rail HAZMAT facilities that ship or receive in an HTUA specified categories and quantities of HAZMAT to appoint a security coordinator and report suspicious incidents.

TSA also proposed clarifying and extending the protections afforded by the sensitive security information (SSI) designation to certain information associated with the rail transportation proposal.

In addition, TSA proposed that freight railroad carriers and the affected rail HAZMAT facilities report to TSA, upon request, the location and shipping information of certain rail cars containing specified categories and quantities of HAZMAT. TSA proposed measures that would ensure a positive and secure exchange of custody and control of rail cars carrying specified categories and quantities of HAZMAT.

3.2.2 Compliance Processes

Compliance programs provide the government with data on industry compliance rates, assist in determining whether security measures are effective at mitigating the identified vulnerabilities, aid in identifying vulnerabilities, and refine consequence

[145] 49 CFR 174.14 and 174.16.
[146] Loaded tank car of TIH, highway route controlled quantity of radioactive material, more than 2,268 kilograms (5,000 pounds) of Class 1.1, 1.2, or 1.3 explosives.

measures. Beginning in October 2006, TSA inspectors began conducting implementation surveys to measure carriers' voluntary adoption of SAIs. In early 2007, TSA will begin inspecting for voluntary adoption of the supplemental SAIs.

Government inspections for regulatory compliance and adoption of voluntary SAIs provide the government with data on the state of railroad security at the facility level, as well as regionally and nationally. An important method for identifying needed improvements in the freight rail mode is to obtain a risk baseline of standing, unattended TIH cars in HTUAs through industry reporting. Through this reporting, the government will monitor industry efforts to lower the baseline risk by 50 percent by the end of 2008 to meet a DHS priority goal. Throughout 2007-2008, the government will encourage practices that lower the number of standing, unattended TIH cars in HTUAs. If through government inspections and industry monitoring, the government determines that the risk-reduction goal is not being met, the government will take stronger action, including strengthening voluntary SAIs or issuing mandatory requirements.

Measurement of Guidance Adoption

TSA uses two methods to measure industry adoption of the SAIs—implementation surveys and traditional inspections.

TSA developed the Implementation Survey program to measure adoption with TSA-issued voluntary standards. Generally, implementation surveys are based on a uniform set of questions designed to illicit a standard set of data. Surveys are primarily conducted by Surface Transportation Security Inspectors (STSIs).

TSA also audits industry adoption of voluntary standards and security practices through the traditional inspection methods of observation and examination of freight rail operations, infrastructure, conveyances, and employees. Currently, TSA implementation audits focus on TIH transporters in HTUAs, and there are plans to survey all HTUAs, Class I carriers, and most short line and regional carriers in 2007.

Regulatory Compliance

FRA has regulatory authority for freight and passenger rail safety. It employs rail inspectors that periodically monitor and enforce the implementation of safety and security regulations on these systems. PHMSA issues safety and security regulations for the transportation of HAZMAT, including transportation by freight rail. Within DHS, CBP enforces numerous regulations issued under various statutes, including, but not limited to, prohibiting illegal activity with regard to aliens, importing and exporting goods, shipping, criminal law, and collecting duties. USCG enforces regulations related to shipping and navigable waters. TSA STSIs enforce regulations issued under TSA authority, including security directives issued for rail and mass transit. Security directives have the force of regulations and remain valid and effective until revised or superseded by subsequent action by TSA.

3.3 Grant Programs

Executive Order 13416 requires the alignment of security grants to assist in implementing security requirements and security guidelines. The Federal Government partnered with the Railroad and Research Foundation (RRF) and provided three grants in 2005 to find better ways to secure the transportation of TIH.

Secure Storage Areas (Safe Havens)

DHS provided $1.5 million to develop performance standards and test a secure storage area prototype on railroad properties. The Safe Havens concept tests combinations of people, processes, and technology security measures that will greatly reduce the likelihood of unauthorized access to rail cars containing TIH at fixed facilities, and increase the security of TIH shipments en route. The requirement for the Safe Haven concept is to define a secure storage area and develop potential solution sets that all

entities—producers and consumers of TIH, rail carriers, and government officials—view as increasing the security afforded to TIH railcars at fixed sites and during shipment.

Rail Corridor Risk Management Tool (RCRMT)

DHS provided $3 million for development and delivery of an RCRMT. The RCRMT is a Web-based risk management tool that the railroad industry, the Federal Government, and other designated entities can use. Using commonly accepted risk management practices, the RCRMT will identify and quantify threat, consequence, and vulnerabilities to produce a definable level of risk. The RCRMT is compatible with the Rail Corridor HAZMAT Response and Recovery Tool (RCHRRT) and with the automatically integrating data that the RCHRRT provides.

Rail Corridor HAZMAT Response and Recovery Tool

DHS provided $500,000 for development and delivery of the tool. The RCHRRT is a Web-based assessment tool that Federal, State, and local governments, and the railroad industry can use. Using a defined protocol and a geographic information system (GIS) interface, the RCHRRT will calculate route-specific HAZMAT risks, assist in route selection decisions, and provide a risk model to identify emergency response requirements. The RCHRRT is compatible with the RCRMT and with the automatically integrating data that the RCRMT produces.

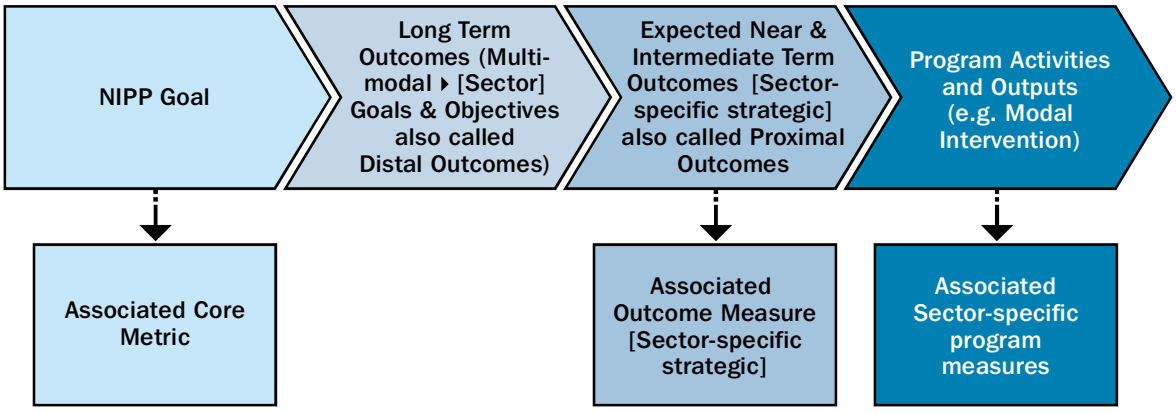
3.4 Metrics

An effective NIPP performance measurement program begins with the collaborative development of metrics to measure progress and performance. This section provides an overview of the plan to implement a Transportation Systems SSP measurement program. Metrics that are developed will supply the data either to affirm that Transportation Systems SSP goals are being met or to show what corrective actions may be required. To be effective, the measurement program will require the cooperation of all modal GCCs and SCCs to provide accurate responses to the metrics being used to measure sector risk posture, SSP effectiveness in the sector, and security program effectiveness. To assess the effectiveness of information-sharing mechanisms on a regular basis, TSA will send quarterly questionnaires to AAR and ASLRRA.

Measurement Working Group. The Freight Rail GCC and invited measurement professionals will initially develop and report on metrics. Under the guidance of TSA's lead measurement organization, the Freight Rail GCC will operationalize measures; establish data sources, data collection, and verification procedures; set measurement policy for the Freight Rail Modal Plan; and approve supporting procedures. This entity may also require standardization of certain measurement practices from data contributors across the freight rail transportation network. The Freight Rail GCC will communicate regularly with Transportation Systems Sector GCC and Freight Rail SCC members and other affected SCCs to ensure that working group progress and plans are fully transparent and coordinated. In addition, work products of the Measurement Joint Working Group will be submitted, when appropriate, to the overarching Transportation Systems Sector GCC/SCC for review.

Measures. The Outcome Monitoring methodology, as shown in figure 3-1, demonstrates working down from the national and multi-modal (sector) goals to determine outcomes and their respective measures.

Figure Annex E3-1: Outcome Model



The Transportation Systems Sector's metrics have been segmented into two categories—core and sector-specific—which are composed of these types of measures:

1. **Core:** As discussed in section 6 of the Transportation Systems SSP, core NIPP metrics are common across all sectors and focus on measuring risk-reduction progress in the sector. These measures are often descriptive statistics (counts).
2. **Sector-Specific:** These metrics are used to gauge the overall effectiveness of the sector toward meeting Transportation Systems SSP goals and objectives. Ordinarily, these are outcome measures capable of quantifying the degree to which the SSP is having an effect on sector security. However, output measures are currently serving as proxies for the long-term outcome measures:
   - Reduce the risk associated with the transportation of TIH in HTUAs by 50 percent by the end of 2008;
   - Number of completed rail corridor assessments on DHS-designated 2006 HTUAs;
   - Percentage of carrier-adopted SAIs; and
   - Percentage of employees who have received security awareness training.

4 Program Management

A subgroup of the Freight Rail GCC will facilitate the coordination and periodic update of this modal plan. The Freight Rail GCC will meet quarterly to address program management issues. The Freight Rail GCC subgroup will coordinate review and update of the plan with the Freight Rail SCC. The Freight Rail GCC will meet biannually with the Freight Rail SCC to address program management issues.

The following is an abbreviated work plan for 2007-2008. TSA programs listed in this section are mostly funded through general operating expenses.

2007

- High Threat Urban Area Rail Corridor Assessments
  – Initiate Baltimore, MD, and Philadelphia, PA
- Comprehensive Reviews
  – Chicago, IL

- TIH Shipment Risk Reduction
  - Set baseline June 2007
  - Observe 25 percent reduction in the risk of TIH transportation by rail by end of 2007
  - Corporate Security Reviews
  - All Class 1
- Hazardous Materials: Enhancing Rail Transportation Safety and Security for Hazardous Materials Shipments NPRM (DOT/PHMSA)
  - NPRM published December 21, 2006
  - Public comment period closed on February 20, 2007
- Rail Security NPRM (DHS/TSA)
  - NPRM published December 21, 2006
  - Public comment closed on February 20, 2007
- Training Course for Railroad Employees: IED Identification Training Video
- TIH Tracking
- Regulatory Compliance Inspections, Implementation Surveys, and Implementation Audits

2008

- High Threat Urban Area Rail Corridor Assessments
  - Complete Baltimore, MD, and Philadelphia, PA
- Corporate Security Reviews
  - Additional HAZMAT carriers
- Training Course for Railroad Employees: Security Awareness Training for All Employees
- TIH Shipment Risk Reduction
  - Continue information collection from railroads
  - Observe 50 percent reduction in the risk of TIH transportation by rail by December 2008
- TIH Tracking
  - Global positioning system (GPS) analysis
- Regulatory Compliance Inspections, Implementation Surveys, and Implementation Audits

5 Security Gaps

Through a process of rail corridor assessments in HTUAs, corporate security reviews, and regulatory enforcement and guidance auditing, TSA has determined that there are three main gaps that threaten the security of the freight rail transportation system and the Nation:

- The presence of standing, unattended, loaded TIH cars in HTUAs presents a significant security gap. These cars pose the greatest risk to the freight rail network and surrounding communities. TSA has undertaken several efforts to close this gap, including issuing SAIs, Rail Transportation Security NPRM, and Rail Corridor Assessments. Most importantly, TSA is partnering with Class I stakeholders to reduce the standing times of these high-risk cars in HTUAs through statistical analysis.
- Although PHMSA has required security plans for shippers and carriers of all HAZMAT in placarded amounts since 2003,[147] there is a lack of robust standardized security planning at the corporate and facility levels for all railroad operations. Through its Corporate Security Review program, TSA is re-evaluating industry security plans and has identified many areas that need improvement. TSA plans to close this gap through robust security measures, which could include possible rulemaking.
- There is a gap in worker security awareness training. Employee training is essential to enhancing the security of the freight rail network because, in most cases, railroad employees are the first line of defense in preventing and detecting acts of terrorism. There are shortcomings in security training, including non-HAZMAT workers, who handle railcars or work at rail facilities. Again, PHMSA has security training requirements for HAZMAT employees;[148] however, PHMSA regulations only require security awareness training[149] and training related to the company security plan.[150] TSA will continue to enhance PHMSA regulations by developing:
  - A training module on identifying IEDs attached to railcars or rail infrastructure to be distributed at no cost to railroads and chemical companies;
  - Guidelines and, if necessary, regulations that build on current requirements; and
  - Training modules to support these standards.

147 See 49 CFR 172.800.
148 HAZMAT employee is defined at id., 171.8.
149 See id., 172.704 (a)(4).
150 See id., 172.704 (a)(5).

Annex F. Pipeline

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, 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 sector is secure, resilient, and able to quickly detect physical and cyber intrusion or attack, mitigate the adverse consequences of an incident, and quickly restore pipeline service.

The Transportation Systems SSP and the Pipeline Modal Annex were developed, reviewed, and updated using both the Transportation Systems Sector and Energy Sector Government Coordinating Council (GCC) and Sector Coordinating Council (SCC) frameworks. In accordance with the National Infrastructure Protection Plan (NIPP), a Critical Infrastructure Partnership Advisory Council (CIPAC) Oil and Natural Gas (ONG) Joint Sector Committee was established to provide a legal framework for members of the Energy Sector GCC and ONG SCC to engage in joint critical infrastructure protection discussions and activities, including those involved with pipeline security. Under this CIPAC committee, a Pipeline Working Group writing team was formed to develop and review applicable SSPs, including the Energy SSP and the Transportation Systems SSP. The writing team reviewed and commented on the draft Transportation Systems SSP Base Plan and drafted the Pipeline Modal Annex. 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) will work with its security partners in both the Transportation Systems and Energy sectors to update the Transportation Systems SSP Base Plan and Pipeline Modal Annex regularly, as called for in the NIPP and Executive Order. The updating process is a responsibility that is shared with pipeline security partners collaboratively through the GCC/SCC/CIPAC framework.

The core of the plan is a pipeline system Relative Risk Assessment and Prioritization methodology. This methodology provides a logical prioritization process to systematically list, analyze, and sort pipeline systems and critical pipeline components within those pipeline systems. By prioritization, security resources can be effectively used to manage risk mitigation in order to protect critical pipelines from terrorist threats. The methodology is based on the Transportation Systems Sector Systems-Based Risk Management (SBRM) methodology, which, in turn, is based on the risk management framework presented in the NIPP.

With a view toward this end-state, the Transportation Systems SSP and this Pipeline Modal Annex focus specifically on how the Transportation Systems Sector will continue to enhance the security of its critical infrastructure and key resources. Programs to

protect the Nation's Pipeline System(s) are key to making the Nation safer, more secure, and more resilient in the face of terrorist attacks and other hazards.

2 Pipeline Overview

2.1 Vision

The Pipeline Modal Annex was developed to ensure the security and resiliency of the pipeline sector. The vision of this plan is to ensure that the pipeline sector is secure, resilient, and able to quickly detect physical and cyber intrusion or attack, 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.

2.2 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 potentially can cause death and injury in 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 based on a collaborative effort between the Federal Government and industry associations.

2.2.1 Types of Pipelines

The following are the main types of pipelines:[137]

1. **Natural Gas Transmission and Storage.** These lines are mostly interstate, transporting natural gas over 310,000 miles of pipeline 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 approximately 160,000 miles of these pipelines in operation, operated by more than 200 operators.

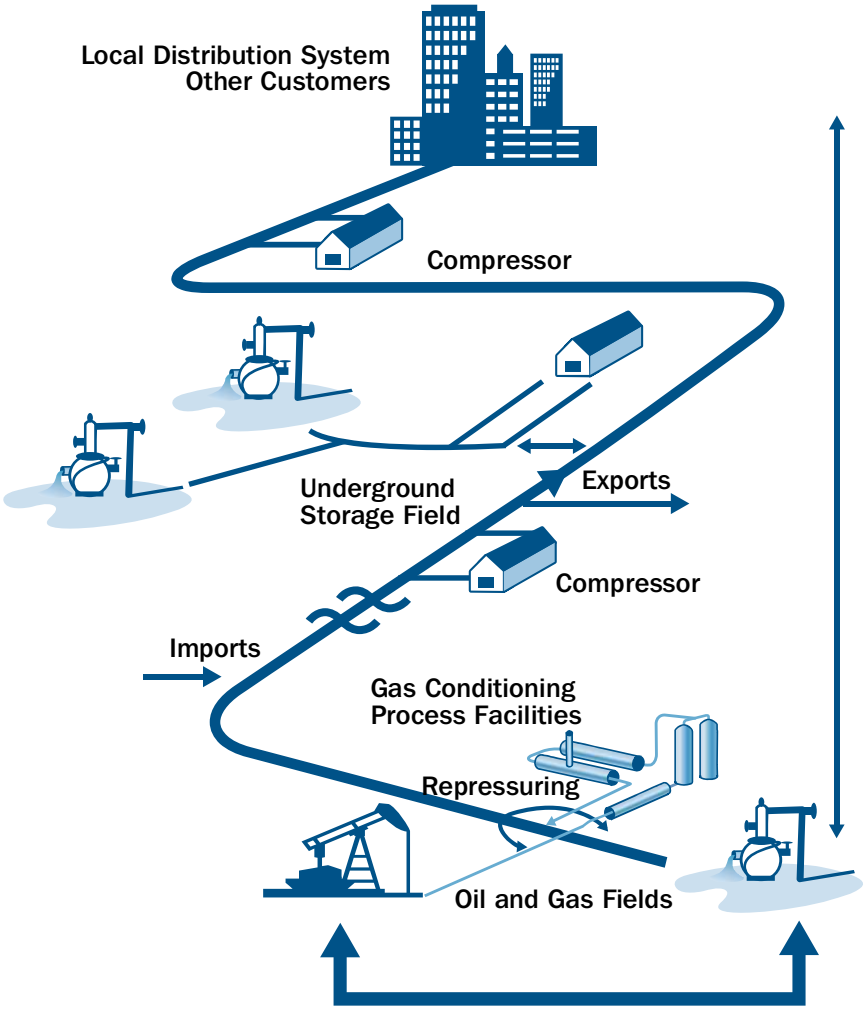
3. **Natural Gas Distribution.** These are typically local distribution company pipelines, mostly intrastate, that transport natural gas from transmission pipelines to residential, commercial, and industrial customers. Included in this segment of the industry are the local distribution companies (i.e., natural gas utilities). More than 1,300 operators operated approximately 1.9 million miles of natural gas distribution pipelines nationwide.

[137] The following sources were used for information in this section: Department of Transportation (DOT) Bureau of Transportation Statistics, DOT Office of Pipeline Safety, Association of Oil Pipelines, American Gas Association, American Public Gas Association, Interstate Natural Gas Association of America.

4. **Liquefied Natural Gas (LNG) Processing and Storage Facilities.** More than 104 facilities nationwide either directly receive LNG from tank ship or truck 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.

Figure F2-1 shows the structure of a typical natural gas pipeline system.

Figure Annex F2-1: Natural Gas Pipeline System



2.2.2 Threats to Pipelines

Oil and gas pipelines have been a favored target of terrorists outside the United States. While there is no specific credible reporting to date indicating that similar attacks will occur in the United States, the fact that terrorist groups have demonstrated the capability and intent to attack pipeline systems abroad raises the possibility that similar attacks could occur inside the United States.

2.3 Government Coordinating Council and Sector Coordinating Council Structure and Process

A Pipeline Working Group has been established to address pipeline issues within the Energy Sector Government Coordinating Council (GCC). Each of the transportation modes is required to have a 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) Sector Coordinating Council (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 Federal Agencies Responsible for Pipelines

Under the NIPP, the TSA is assigned as a Sector-Specific Agency (SSA) for the Transportation Systems Sector, including the pipeline systems mode. The U.S. Coast Guard (USCG) 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 coordinate on matters related to transportation security and transportation infrastructure protection. The Department of Justice (DOJ) 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 and key resources (CI/KR) in collaboration with the Department of Homeland Security (DHS).

2.5 Information Sharing

A number of methods have been employed and will continue to be used to foster good communications and information sharing within the pipeline mode.

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, TSA 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. Unscheduled 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: the American Petroleum Institute (API), Association of Oil Pipe Lines (AOPL), Interstate Natural Gas Association of America

(INGAA), American Gas Association (AGA), and American Public Gas Association (APGA). These associations can quickly pass information to their member companies, as demonstrated by the numerous conference call information-sharing sessions conducted with their respective security committees over the past 5 years.

Homeland Security Information Network

The Homeland Security Information Network (HSIN) is an Internet-based communications system established by the DHS to facilitate information exchange between the DHS and other government, private sector, and nongovernmental organizations involved in antiterrorism and incident management activities. In May 2006, the ONG SCC signed a Memorandum of Understanding (MOU) with the DHS to establish the ONG HSIN. Efforts are underway to incorporate pipeline security communications and information-sharing activities into the existing HSIN system. Once completed, the pipeline mode will use the ONG HSIN.

Federal Energy Regulatory Commission (FERC) Pipeline Engineering Data and Damage Reporting

FERC has taken steps to provide the relevant engineering data that it receives from jurisdictional interstate pipelines in the context of location siting and permitting to DOE. In June 2006, 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.

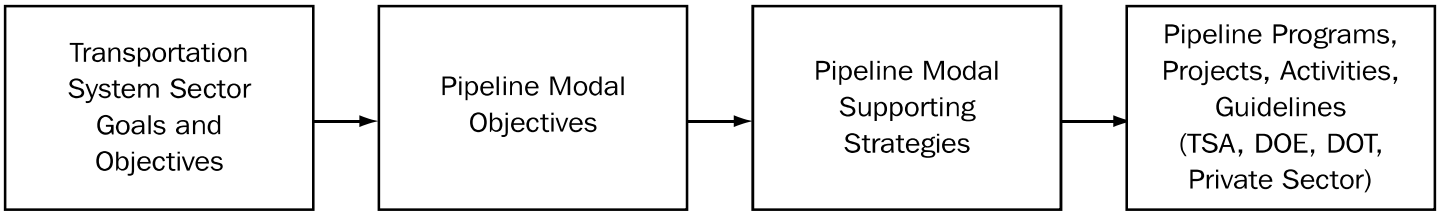
3 Implementation Plan

3.1 Goals, Objectives, and Programs/Projects/Activities

Three overarching Transportation Systems Sector security goals and 10 supporting objectives reflect the goals stated in the NIPP. The Pipeline Modal Annex outlines three objectives that aim to achieve the Transportation Systems 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 combined contributions of the TSA Pipeline Security Division and other Federal, State, local, and private sector security partners and reflect the significant efforts of all pipeline stakeholders to secure our Nation's pipeline systems.

Figure F3-1 shows the relationship 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 Annex 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. Refer to appendix 1 for 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 Sector Goals and Supporting Objectives

The following are the Transportation Systems Sector overarching goals and their supporting objectives:

1. **Prevent and deter acts of terrorism using or against the transportation system.**
   Supporting sector objectives:
   - 1A. Implement flexible, layered, and effective security programs using risk management principles;
   - 1B. Increase the vigilance of travelers and transportation workers; and
   - 1C. Enhance information and intelligence sharing among Transportation Systems Sector security partners.
2. **Enhance the resiliency of the U.S. transportation system.**
   Supporting sector objectives:
   - 2A. Manage and reduce the risk associated with key nodes, links, and flows within critical transportation systems to improve overall network survivability; and
   - 2B. Ensure the capacity for rapid and flexible response and recovery to all-hazards events.
3. **Improve the cost-effective use of resources for transportation security.**
   Supporting sector objectives:
   - 3A. Align sector resources with the highest priority transportation security risks using both risk and economic analysis as a decision criteria;
   - 3B. Ensure robust sector participation as a partner in developing and implementing public sector programs for CI/KR protection;
   - 3C. Improve the coordination and risk-based prioritization of Transportation Systems Sector security research, development, test, and evaluation (RDT&E); and
   - 3D. Align risk analysis methodologies with the Risk Analysis and Management for Critical Asset Protection (RAMCAP) criteria outlined in the NIPP.

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 CI/KR vulnerabilities against threats and natural perils.
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 the effects of **terrorist attacks** or natural disasters.
3. **Increase the level of domain awareness and information sharing and response planning and coordination** through enhanced training, network building, and efficient research and development (R&D) application.

These three modal objectives, which emanate from the NIPP, directly support the Transportation Systems Sector goals and are aligned with the applicable pipeline portions of the Energy Sector goals as stated in the Energy SSP.

While no specific objective is directed at achieving the "cost-effective use of resources" as stated in the sector goals, 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 benefit analysis and maximize 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 below. The programs, projects, and activities are listed below, along with a brief description and the function and corresponding strategies that they support. The following are the modal strategies:

1. **Promote the implementation of layered threat deterrence and vulnerability mitigation programs** in pipeline systems and CI/KR, 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 planning 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 CI/KR 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 of 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 role/responsibility among pipeline security partners.
7. **Conduct R&D and other activities** that build domain awareness in all facets of risk mitigation and resiliency enhancement through coordinated and efficient use of assets.

3.1.4 Pipeline Programs, Projects, and Activities

The tables in sections 3.1.4.1 through 3.1.4.3 present the programs, projects, and activities (either already undertaken or planned) that promote prevention; deterrence; preparedness; system resiliency; and information sharing for physical, cyber, and human 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, the pipeline modal strategies that each support, and describe the security facets (e.g., cyber security, physical infrastructure security).

3.1.4.1 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 Corporate Security Review (CSR) programs. These two programs are briefly described in this section; however, more details can be found in section 4.

Program/Project/Activity	Description	Participants	Strategies Supported	Facets
Pipeline System Relative Risk Ranking and Prioritization Tool	Statistical data used to perform relative risk ranking and prioritize CSR findings	TSA, Industry	2, 7	C, H, P
Pipeline CSR Program	On-site security reviews of pipeline company security	TSA, Industry	1, 6	C, H, P, I, N
Cyber Attack Awareness	Training and presentations on Supervisory Control and Data Acquisition (SCADA) vulnerabilities	TSA, GTI	1, 3, 5, 7	C, I
Landscape Depiction and Analysis Tool	Incorporates combined graphic and written descriptive depiction of the pipeline domain, with risk analysis components	TSA	2, 7	C, H, P
Pipeline Cross-Border Vulnerability Assessment Program (International)	U.S. and Canadian teams assess pipeline operations, control systems, interdependencies, and assault planning in critical cross-border infrastructure	TSA, Natural Resources Canada	1, 2, 5	I, N, P, S
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	I, N, S
G8 Threat, Vulnerability, and Contingency Planning for Critical Pipeline Infrastructure (International)	Multi-national sharing of threat assessment methodology; advisory levels and effective practices and vulnerability assessment information; also develops a G8-based contingency planning guidance document	TSA, DHS, DOS, G8 Member Nations	6	C, H, I, N, P, S
Pipeline Policy and Planning	Coordination, development, implementation, and monitoring of national and TSA pipeline planning	TSA, DHS, DOT, DOE	4, 6	N, S
Regional Gas Pipeline Studies	Regional natural gas supplies studies for key markets nationwide	TSA, DOE, INGAA, GTI, NETL, Industry	2, 7	D, S
Security Awareness Training Compact Discs (CD)	Informational CDs about pipeline security issues and improvised explosive devices (IED)	TSA	1, 2, 6	S
TSA Pipeline Security Stakeholder Conference Calls	Periodic information-sharing teleconference calls between TSA, government, and industry security partners	TSA, Other Government Agencies, Industry	6	N, S

Program/Project/Activity	Description	Participants	Strategies Supported	Facets
Transportation 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	N, S
Pipeline Blast Mitigation Studies	Research test, including explosive tests on various configurations of pipe to determine resiliency characteristics	TSA, DoD, Transportation Systems Sector Working Group	1, 4, 7	D, P, R
2006 Virtual Library Pipeline Site Development	TSA Web portal for information-sharing purposes	TSA	6	S

Legend for Facets Column

C = Cyber Infrastructure	D = Research and Development	H = Human Infrastructure
I = International	N = Network Building	P = Physical Infrastructure
R = Resiliency Enhancing	S = Information Sharing	

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

Program/Project/Activity	Description	Participants	Strategies Supported	Facets
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	S
Homeland Security Advisory System (HSAS)	Information-sharing program that makes government, the private sector, and the public more vigilant when credible threat information becomes available	DHS	1, 6	S
Lessons Learned Information Sharing (LLIS)	Information clearinghouse and knowledge base	DHS	3, 4, 6	S
Visualization and Modeling Working Group	Identifies risks and industry needs to improve secure control systems	DOE, DHS, Canada, Industry	4, 7	S
DOT, DOE, DHS Incident Drill Programs/Sponsorship and Participation	Tabletop and field exercises facilitation	DOT, DOE, DHS, PHMSA	3, 4	N, R

Program/Project/Activity	Description	Participants	Strategies Supported	Facets
DOT Emergency Response and DOT-Sponsored Training/Workshops	Incident response training and pipeline incident response field representatives for contingency planning, resiliency, and restore and repair capabilities	DOT, PHMSA	4, 5	R, S

3.1.4.3 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 just a small sample of the industry's programs, projects, and activities that support the pipeline modal objectives.

Program/Project/Activity	Description	Participants	Strategies Supported	Facets
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	N, S
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	N, R
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	N, S
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	C, H, P, S
API Security Committee and AGA Security Committee-Sponsored Training and Workshops	Workshops/forums and training for gas and liquid petroleum industry	API	5, 6	S

Program/Project/Activity	Description	Participants	Strategies Supported	Facets
Pipeline Company Security Protective and Deterrence Measures	Pipeline operators have been enhancing protective and deterrence measures in accordance with the 2002 Pipeline Security Circular	Pipeline Companies	1	C, H, P

3.2 Pipeline Security Smart Practices, Security Guidelines, Security Standards, and Compliance and Assessment Programs

Various smart practice documents, guidelines, and standards have been developed and implemented within the pipeline mode that support the modal objectives. These efforts are described in the tables below.

3.2.1 TSA Smart Practices, Guidelines, Standards, and Programs

Practices/Guidelines/ Standards/ Program	Description	Participants	Strategies Supported	Facets
Pipeline Security Smart Practices	Document to assist hazardous liquid and natural gas pipeline industries in their security planning and implementation	TSA, Industry	1, 4	C, H, P, S
2002 DOT Pipeline Security Guidelines	Guidelines that suggest minimum security levels for prevention, deterrence, and security incident response	TSA, DOT	1, 6	C, H, P, S

3.2.2 Industry Smart Practices, Guidelines, Standards, and Programs

Practices/Guidelines/Standards/ Program	Description	Participants	Strategies Supported	Facets
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, cyber security, and relevant operational standards	AGA, INGAA, APGA	1	C, H, P, S
Cryptographic Protection of Supervisory Control and Data Acquisition (SCADA) Communications	Define encryption methods for SCADA systems	AGA	1	C, R

Practices/Guidelines/Standards/ Program	Description	Participants	Strategies Supported	Facets
API Security in the Petroleum Industry: Practices Guidelines	Recommend security practices for all segments of liquid and gas petroleum industry	API	2	C, H, P
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	C, S
API Information Management and Technology Program	Provide a comprehensive review and quantitative assessment of company security programs	API	2	C, S

3.3 Federal Grant Programs

The following Federal grant program supports the pipeline modal objectives and strategies.

Program/Project/Activity	Description	Participants	Strategies Supported	Facets
Buffer Zone Protection Program	Provide resources to identify and mitigate the vulnerabilities of critical infrastructure	Federal, State, local governments; Industry	1, 7	P, R

3.4 The Way Forward

TSA will continue to participate in all aforementioned programs, projects, and activities. However, the core of TSA's efforts is the CSR process and the Pipeline System Relative Risk Assessment and Prioritization methodology, which will continue to grow year by year. These efforts are described in greater detail in section 4.

In addition, TSA plans to address needed improvements and gaps in the following areas to improve security awareness.

International

The relationship with Canada has proven to be extremely worthwhile and the plan is to establish a working relationship and program within fiscal years (FYs) 2007 and 2008.

National

Although progress has been made in establishing roles and responsibilities with government and industry partners, further definition and programs must be established. The sector partners need to expand to other State, regional, and tribal governments, and industry. These programs need to be established in FYs 2007, 2008, and 2009.

Training and Exercises

Industry partners have established security training programs and TSA has produced and distributed a training compact disc (CD). However, there are no training standards established, and many aspects of the sector are not involved in any training programs. These programs are under development and will be expanded in each fiscal year as appropriate.

4 Risk-Based Approach to Pipeline Security

This section is included to provide details on how TSA will use risk-based programs to achieve the overarching Transportation Systems Sector goals. It should be noted that it deviates from the model that the other modal annexes followed. "Program Management" is found instead in section 5.

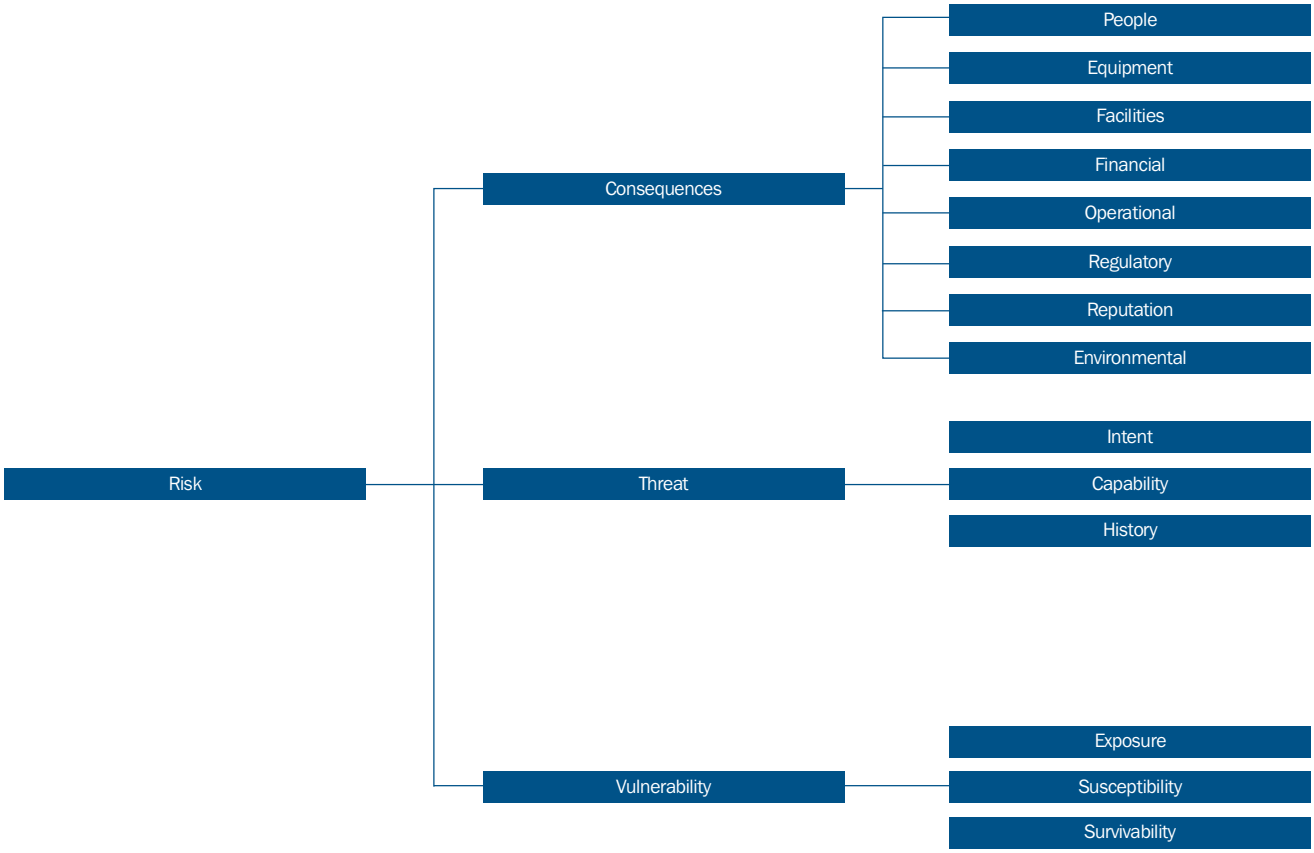
4.1 Defining and Measuring Risk

In practical terms, a risk-based approach to security is recognizing that there are too many risk scenarios to protect all risks equally, so we have to establish priorities and allocate security resources accordingly. A more theoretical description of risk is that it is a function of likelihood (mathematically expressed as a probability) multiplied by the consequences (in terms of people, facilities, financial loss, operational disruption, etc.). Likelihood can be further broken down into threat (an adversary's capability + 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. We try to measure the various parts of risk for which information is available and make some judgment calls where it is not.

Figure F4-1 shows the framework that will be used to define risk for the purposes of this approach.

Figure Annex F4-1: Risk Definition Framework



The TSA Pipeline Security Division relies on TSA's Office of Intelligence to provide threat assessments based on information received from the Intelligence Community, including the FBI, Central Intelligence Agency (CIA), the DHS Office of Intelligence and Analysis (I&A), and others. When there is specific threat information about a pipeline facility or system, the TSA Pipeline Security Division will enlist the aid of TSA's Office of Law Enforcement to conduct a joint vulnerability assessment of the targeted facility and provide the report, with options for consideration, to the pipeline operator. These joint vulnerability assessments (JVAs) are done in concert with representatives from other parts of the DHS, as well as the local Joint Terrorism Task Force (JTTF).

4.2 Pipeline System Relative Risk Assessment and Prioritization

The natural gas and hazardous liquids pipeline system infrastructure is a large, widely dispersed, and mostly privately owned system. While there is a desire to secure all aspects of all critical infrastructures, the total pipeline system universe 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 Assessment and Prioritization methodology that provides a logical prioritization process is required to list systematically, analyze, and sort pipeline systems and critical pipeline components within those pipeline systems. TSA will do the prioritization exclusively with input from pipeline operators and industry trade associations. Through prioritization, government security resources can be used effectively to manage risk mitigation to protect critical pipelines from terrorist threats. Pipeline systems will always be ranked and evaluated first before any specific asset or component. The overall guidance for the methodology is introduced in section 3.2 of the Transportation Systems SSP.

Individual pipeline companies will conduct Security Risk Analysis on their corporate assets. Reasonable security 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.

4.3 Pipeline Relative Risk Ranking

In the case of the pipeline industry, the overarching objective is to protect crucial energy supply to commercial, industrial, and domestic users. The process requires a strong understanding of the pipeline industry. The objective is to focus attention on the pipeline systems that, if damaged, could have the greatest impact on energy supplies and national security.

In the first step, TSA 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.

4.4 System Screen and Asset Identification

TSA will continue to gather data by conducting CSRs in cooperation with sector security partners to further evaluate and categorize pipeline systems. The CSR program has gathered excellent pipeline system data since its inception 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 that can be evaluated both quantitatively and qualitatively to further prioritize critical pipeline systems.

During the CSR process, potentially critical assets are examined and cataloged based on their importance to the pipeline systems. Assets are identified and a link between the asset and the critical pipeline system will be 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 above-ground piping; and
- Storage facilities.

In addition to the above, TSA is sponsoring regional gas studies of key markets in the United States in cooperation with DOE. These studies, which have been ongoing since 2003, improve our understanding of which regions are most vulnerable to gas supply disruptions, and they provide a sense of what the consequences of those disruptions might be. TSA will continue to evaluate pipeline networks comprised of separate pipeline systems or companies serving a region (the Northeastern United States, the west coast, etc.). Regional criticality can vary depending on seasonal usage, weather, or other factors, but will be evaluated based on worst case scenarios. TSA also examines high-level dependencies and interdependencies with other regions and systems. Pipelines serving regions with critical needs and greater vulnerability will be ranked higher in the screening process.

4.5 Detailed System and Asset Assessment (Future State)

In the future, TSA plans to conduct more detailed System and Asset Assessment programs. Private pipeline sector 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 an asset, system, or network'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 resiliency 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 cyber security for Supervisory Control and Data Acquisitions (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, federally 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 in current use and each varies in the assessment approach. RAMCAP, Site Assistance Visits (SAVs), and TSA's JVAs are examples of field assessment tools. As outlined in the NIPP, flexibility in the approaches taken is given as long as it conforms to the basic criteria outlined in the NIPP.

Assessment teams will perform on-site facility security evaluation of several items, including:

- Access control;
- Closed-circuit television (CCTV) and intrusion detection systems;
- Barriers and fencing;
- Power supply and backup generators;
- Telecommunications and other interdependencies;
- On-site security personnel; and
- Local law enforcement and emergency response resources.

4.6 Prioritization

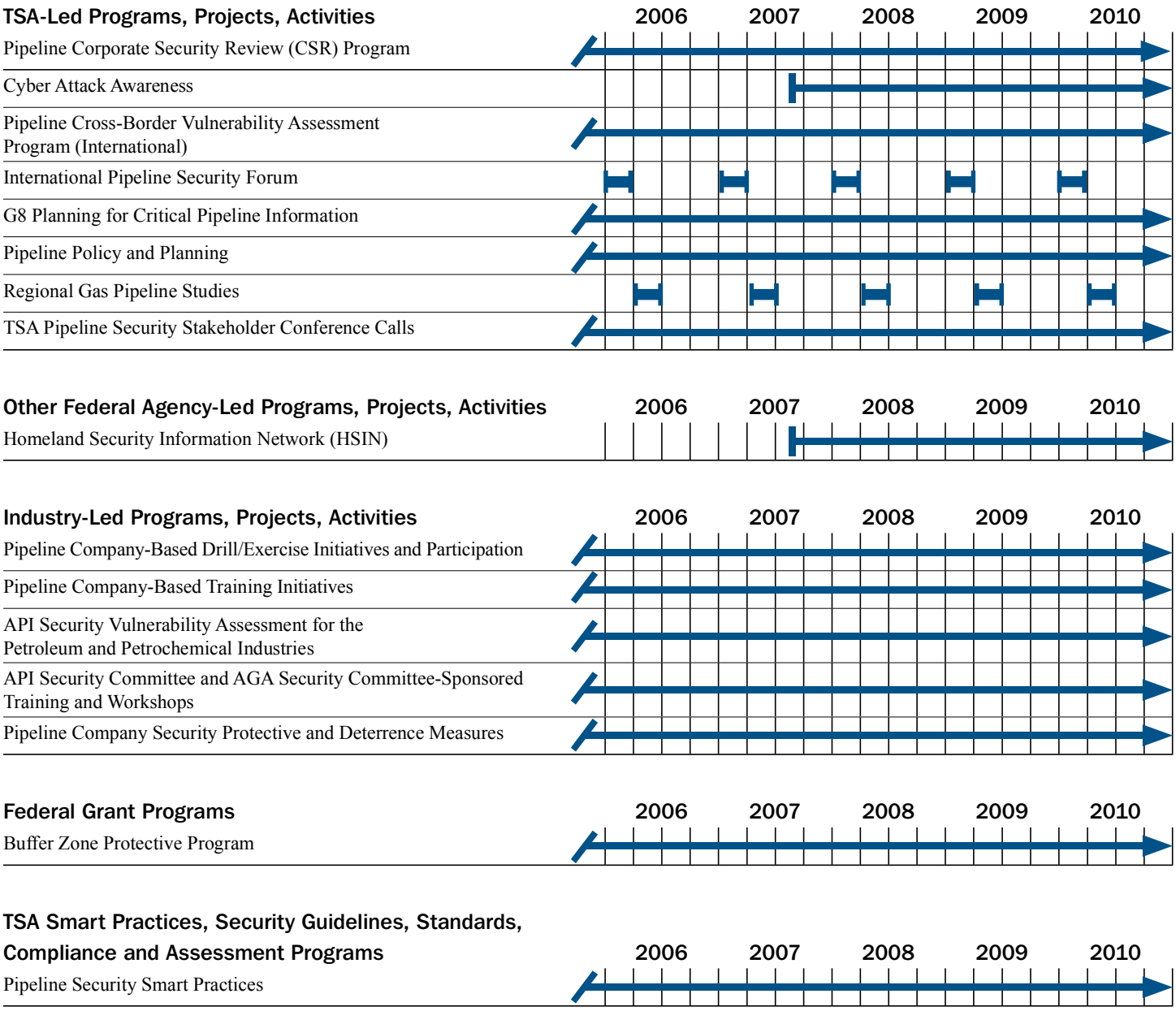
TSA will use a pipeline system Relative Risk Assessment and Prioritization methodology to rank the most critical systems and assets according to the greatest importance to energy supplies and risk with regard to threat, vulnerability, and consequences. The list will be sorted using proven qualitative 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. In the future, within each assessed pipeline system, individual component assets will be also ranked in the same manner. With periodic re-evaluation, the ranking list will probably change over time. In addition, subject matter experts will use their knowledge to verify the algorithm's results.

5 Pipeline Security Program Management

TSA uses the GCC/SCC/CIPAC framework to develop and coordinate program activities. To enable participation of government and industry stakeholders, TSA conducts monthly conference calls, visits pipeline operators periodically to conduct CSRs, and participates in GCC and CIPAC meetings. TSA and DOT's Pipeline and Hazardous Materials Safety Administration (PHMSA) have jointly developed a pipeline annex to the DOT/DHS MOU to further clarify their roles in pipeline security and safety, respectively.

The following charts show the implementation timelines for the program activities that are designed to identify and address gaps in pipeline security.



6 Security Gaps

The following is a list of security gaps that are currently being addressed in each of the programs listed in section 3.1.4 of this annex.

1. The TSA Pipeline Security Division conducts CSRs to assess pipeline security. The intent of these on-site security reviews of pipeline companies is to develop firsthand knowledge of security planning and execution at critical pipeline systems, establish communications with key pipeline security personnel, and identify and share smart practices. As industry-wide security gaps are identified through the CSR process, the TSA Pipeline Security Division develops programs to address gaps throughout the pipeline industry.
2. 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 infra-

structure and identify additional necessary protective measures. In the area of pipeline security, the TSA Pipeline Security Division has partnered with Natural Resources Canada to conduct system assessments. Four pipeline systems have been reviewed by a joint U.S./Canadian team, the most recent in June 2006. It is planned to conduct an additional system assessment this year.

3. While the security of individual pipeline systems has been addressed, regional studies evaluating potential service disruptions have not been conducted. To address this problem, regional gas studies are being conducted. These projects assess the capabilities and resiliencies of the Nation's natural gas delivery infrastructure to withstand service disruption and examine the range of implications in the event of a natural gas disruption. The studies, conducted by contractor staff, develop information and analyses to allow Federal and State agencies and other interests to develop effective security policies and restoration plans to ensure natural gas deliveries in the face of potential disruptions. The TSA Pipeline Security Division is a member of the Steering Council for this project.

4. 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 a training CD. 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. The TSA Pipeline Security Division has worked with industry partners to develop the training CD for distribution to pipeline stakeholders.

5. Due to industry dependence on remote-control systems, cyber threats continue to be an area of concern. The TSA Pipeline Security Division has two programs and objectives that address this gap. First, SCADA systems are used by the pipeline industry to monitor and remotely control their pipelines. It is technically possible for hackers, terrorists, or foreign governments to access these SCADA systems to obtain confidential information and/or damage the systems using the remote control. TSA partnered with the Gas Technology Institute (GTI) to develop presentation materials to illustrate existing SCADA vulnerabilities and consequently increase the cyber security awareness of pipeline companies. Second, SCADA systems are increasingly important to the operation of the Nation's pipelines. A program of SCADA security evaluation is a necessary addition to the TSA Pipeline Security Division's CSRs in order to assess the vulnerability of these networks to cyber attack. This program is intended to become an adjunct to the CSR program. It will continue on an ongoing basis.

6. To ensure continued domain awareness and information sharing, the TSA Pipeline Security Division conducts an annual pipeline international forum, hosts monthly conference calls, provides suspicious incident reports to the industry, actively participates in the industry GCC and SCC, and plans to revise the pipeline security guidelines.

Appendix 1: Objectives/Strategies/Programs/Goals Alignment Table

Pipeline Modal Objectives	Supporting Strategies	Supporting Programs, Projects, Activities, Guidelines, etc.	Transportation Systems SSP Objectives Supported
1. Reduce level of risk through analysis and implementation of security programs that enhance deterrence and mitigate CI/KR vulnerabilities against threats and natural perils.	(1) Implement layered threat deterrence and vulnerability mitigation programs.	Cyber Attack Awareness; Pipeline Cross-Border Vulnerability Assessment Program; Pipeline Corporate Security Review (CSR) Program; Security Awareness Training CD; Pipeline Security Smart Practices; Pipeline Blast Mitigation Studies	1A. Implement flexible, layered, and effective security programs using risk. 2A. Manage and reduce the risk associated with key nodes, links, and flows within critical transportation systems to improve overall network survivability. 3A. Align sector resources with the highest priority transportation security risks using both risk and economic analysis as decision criteria.
	(2) Develop and perform collaborative risk analysis processes.	Landscape Depiction and Analysis Tool; Pipeline Cross-Border Vulnerability Assessment Program; Regional Gas Pipeline Studies; Pipeline System Relative Risk Ranking and Prioritization Tool	3B. Ensure robust sector participation as a partner in the development and implementation of public sector programs for CI/KR protection. 3D. Align risk analysis methodologies with the Risk Analysis and Management for Critical Asset Protection (RAMCAP) criteria outlined in the NIPP.
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 the effects caused by terrorist attacks or from natural perils.	(3) Use collaborative plan development and drill/exercise participation.	Pipeline Security Regulations 193.2900, 193.2905/NFPA 59A; DOT-Sponsored Exercises; Company-Based Drill/Exercise Participation; Lessons Learned Information Sharing (LLIS)	2A. Manage and reduce the risk associated with key nodes, links, and flows within critical transportation systems to improve overall network survivability. 2B. Ensure the capacity for rapid and flexible response and recovery to all-hazards events. 3A. Align sector resources with the highest priority transportation security risks using both risk and economic analysis as decision criteria. 3B. Ensure robust sector participation as a partner in the development and implementation of public sector programs for CI/KR protection.
	(4) Promote pipeline system resiliency and contingency capability enhancement measures.	G8 Threat, Vulnerability, and Contingency Planning for Critical Pipeline Infrastructure; Pipeline Policy and Planning; Pipeline Blast Mitigation Studies	
	(5) Conduct security-related training that enhances domain awareness.	DOT-Sponsored Contingency, Resiliency, Response, Restore Training/Workshops	

Pipeline Modal Objectives	Supporting Strategies	Supporting Programs, Projects, Activities, Guidelines, etc.	Transportation Systems SSP Objectives Supported
3. Increase the level of domain awareness, information sharing, and response planning and coordination through enhanced training, network building, and efficient R&D application.	(5) Conduct security-related training that enhances domain awareness.	DOT-Sponsored Contingency, Resiliency, Response, Restore Training/Workshops; Security Awareness Training CD; API/AGA Workshops	1B. Increase vigilance of travelers and transportation workers 1C. Enhance information and intelligence sharing among transportation sector security partners. 3A. Align sector resources with the highest priority transportation security risks using both risk and economic analysis as decision criteria. 3B. Ensure robust sector participation as a partner in the development and implementation of public sector programs for CI/KR protection. 3C. Improve the coordination and risk-based prioritization of transportation sector security Research, Development, Test, and Evaluation (RDT&E).
	(6) Conduct network enhancement and information-sharing activities.	Cyber Attack Awareness; Pipeline Cross-Border Vulnerability Assessment Program; CSR Program; International Pipeline Security Forum; G8 Threat, Vulnerability, and Contingency Planning for Critical Pipeline Infrastructure; Pipeline Policy and Planning; Security Awareness Training CDs; Pipeline Security Smart Practices; TSA Pipeline Security Stakeholder Conference Calls; Virtual Library Pipeline Site Development; Pipeline Company-Based Security Training Initiatives	
	(7) Conduct R&D and other activities that build domain awareness.	Cyber Attack Awareness; Landscape Depiction and Analysis Tool; Regional Gas Pipeline Studies; Pipeline System Relative Risk Ranking and Prioritization Tool; Pipeline Blast Mitigation Studies	

Appendix 2: Descriptions of Programs, Projects, Activities, Guidelines, and Standards

TSA-Led Programs, Projects, and Activities

Pipeline System Relative Risk Ranking and Prioritization Tool

This program and associated activities are currently being developed within TSA. It compiles statistical data on pipeline systems that will be used to perform a relative risk ranking and to prioritize CSR results/findings to maximize focus and direction of resources toward these areas. This program supports strategies 2 and 7.

Pipeline CSR Program

Since 2003, TSA has been conducting CSRs and on-site security reviews 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. This program supports strategies 1 and 6.

Cyber Attack Awareness

TSA is partnering with GTI to develop training and presentation materials to illustrate existing SCADA vulnerabilities and consequently increase the cyber security awareness of pipeline companies. This program supports strategies 1, 3, 5, and 7.

Landscape Depiction and Analysis Tool

Currently under development, this tool incorporates a combined graphic and written descriptive depiction of the pipeline domain. It is also a risk analysis tool that can be used in the analysis of threats, vulnerabilities, and consequences (TVC) as they are related to specific types of pipeline facilities within a system. This program supports strategies 2 and 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 of North America 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. This program supports strategies 1, 2, and 5.

International Pipeline Security Forum

TSA, in conjunction with Natural Resources Canada, annually hosts the International Pipeline Security Forum. This international forum provides an opportunity for the U.S. and Canadian governments and industry pipeline officials to discuss security issues and topics. This program supports strategies 5 and 6.

G8 Threat, Vulnerability, and Contingency Planning for Critical Pipeline Infrastructure (International)

This three-piece project includes forming consensus on determining threat methodologies for critical pipeline infrastructure, forming consensus on effective practices associated with conducting vulnerability assessments of pipelines and critical nodes/facilities, and developing a G8-based contingency planning guidance document that provides practices and approaches used to protect /secure critical pipeline infrastructure against the threat of terrorism. Components of TSA are working closely with both the Department of State and DHS headquarters to develop a contingency guidance document that provides smart practices and approaches for protecting and securing critical pipeline infrastructure against terrorist threats. Member States may use this information to prepare and implement effective security measures and better respond to specific threat conditions. This program supports strategy 6.

Pipeline Policy and Planning

TSA, in collaboration with other Federal and private industry security partners, coordinates, develops, implements, and monitors national and TSA-specific plans such as the Transportation Systems SSP, Performance Assessment and Rating Tool (PART), National Asset Database (NADB), and Continuity-of-Operations Plans (COOPs). TSA participates in DHS planning activities such as the TSA strategic, acquisition, and business planning activities, and monitors their performance. Additionally, TSA imple-

ments and manages planning, metrics, and milestones, and coordinates with the other transportation modes, as well as other DHS and interagency threat and risk-based planning efforts such as the Strategic Homeland Infrastructure Risk Assessment (SHIRA) and event-driven risk analysis. This program supports strategies 4 and 6.

Regional Gas Pipeline Studies

TSA, in cooperation with DOE, is sponsoring a study of regional natural gas supplies for key markets nationwide. These studies, which have been ongoing since 2003, use computer-based modeling to evaluate the impact of a major pipeline disruption as the result of a terrorist attack. As of 2006, most regions of the country have been evaluated. The prime contractor for the effort is the National Energy Technology Laboratory; GTI does the technical analysis with support from Science Applications International Corporation (SAIC). This program supports strategies 2 and 7.

Security Awareness Training Compact Discs

TSA developed two CDs for distribution to pipeline transmission and distribution companies. The general focus of the CD is toward stakeholders and their employees who have the need for a basic level of awareness and understanding of pipeline security. A more in-depth security awareness CD was also developed for those whose responsibilities include or greatly affect pipeline security, such as security personnel. This CD focuses on more in-depth analysis of the terrorist mindset and characteristics and improved identification of improvised explosive devices (IEDs) and vehicular-borne improvised explosive devices (VBIEDs). In addition, this CD contains other informational "tools" that would be of assistance in pipeline security. This program supports strategies 1, 2, and 6.

TSA Pipeline Security Stakeholder Conference Calls

See section 2.5 for information on these regularly scheduled calls. This program supports strategy 6.

2006 Virtual Library Pipeline Site Development

Currently under development within TSA, this project and its related activities will create a TSA Pipeline Security informative Web site in the TSA Virtual Library for information sharing among pipeline modal stakeholders and other transportation mode personnel within TSA. This program supports strategy 6.

Pipeline Blast Mitigation Studies

This is a research test project involving the multi-agency Technical Support Working Group (TSWG), DoD, and TSA. The project entails conducting explosive tests on various configurations of pipe to determine resiliency characteristics. This program supports strategies 1, 4, and 7.

Other Federal Agency-Led Programs, Projects, and Activities

Homeland Security Information Network (HSIN)

HSIN is an information-sharing tool that the DHS Infrastructure Protection Office developed in partnership with the private sector that provides a secure/non-secure Web-based source for security-related information, threat intelligence, and indications and warnings. This program supports strategy 6.

Homeland Security Advisory System (HSAS)

HSAS is an information-sharing program that improves security by making government, the private sector, and the public more vigilant when credible threat information on terrorist activity or intentions becomes available. The DHS is responsible for system operation, including intelligence assessment, setting appropriate HSAS level, educating users about the system, and disseminating advisories through multiple media. This program supports strategies 1 and 6.

Lessons Learned Information Sharing (LLIS)

The DHS facilitates the LLIS program, which entails an information clearinghouse and knowledge base that promotes dissemination of vetted, static-type reference information, standards, guidelines, lessons learned, and best practices to the transporta-

tion stakeholder community while maintaining adherence to consistent, systematic DHS vetting criteria. By promoting awareness of threats and transportation security vulnerabilities, LLIS will enable an agile incident-response capability for stakeholders through promoting programs, processes, and activities that enhance security. This program supports strategies 3, 4, and 6.

Visualization and Modeling Working Group

The Visualization and Modeling Working Group is a joint program among the DHS, DOE, Public Safety Emergency Preparedness Canada, Natural Resources Canada, and the private sector that identifies risks and industry needs to improve secure control systems. This program supports strategies 4 and 7.

DOT Incident Drill Programs/Sponsorship and Participation

The DOT Pipeline and Hazardous Materials Safety Administration (PHMSA) Office of Pipeline Safety (OPS) leads tabletop and field exercises with Federal, State, local, and tribal environmental protection, law enforcement, emergency management, public, media, and energy industry representatives. PHMSA OPS helps design, conduct, and evaluate exercises with government, public, and industry partners. This program supports strategy 3.

DOT Emergency Response and DOT-Sponsored Training/Workshops on Contingency Planning, Resiliency, Emergency Response, and Restore and Repair Capabilities

PHMSA serves on the National Coordinating Committee with USCG, the Minerals Management Service, and the Environmental Protection Agency (EPA). The committee seeks to better protect people and the environment from oil spills. PHMSA trains representatives in the National Incident Management System (NIMS), Unified Command, emergency communications, and hazardous waste operations and emergency response (HAZWOPER). PHMSA representatives work in the field and in the Crisis Management Center to respond to natural and manmade disasters that may involve pipelines. This program supports strategies 4 and 5.

Pipeline Industry-Led Programs, Projects, and Activities

Pipeline Company-Based Security Training Initiatives

Security awareness and training are elements included in Federal Government and industry guidelines. Initiatives include corporate and field training and usually include response measures tied to the DHS Homeland Security Advisory System. Tools include briefings, manuals, CDs, and computer-based training. This program supports strategy 5.

Pipeline Company-Based Drill/Exercise Initiatives

Since 2002, at both the regional and national levels, pipeline operators have been participating in drills/exercises related to infrastructure security at all levels (Federal, State, regional, local, and corporate). Since energy is a critical infrastructure and a key player in interdependencies with other sectors of the economy, pipelines have engaged in tabletop and on-site simulated exercises. These include terrorist and natural disaster scenarios. Since most operators are regulated at the State level, this includes drills/exercises by State commissioners and Governors. This program supports strategy 3.

API/NPRA Security Vulnerability Assessment for the Petroleum and Petrochemical Industries

This informative and instructional guide provides practical hands-on knowledge for performing security vulnerability assessments in multiple petroleum and petrochemical-related industries. This program supports strategy 2.

API Security Committee and AGA Security Committee-Sponsored Training and Workshops

Each association's related security committees hold workshops/forums and training for the gas and liquid petroleum industry to discuss/share information and educate members on security-related issues. This program supports strategies 5 and 6.

Pipeline Company Security Protective and Deterrence Measures

Since the issuance of and in accordance with the 2002 Pipeline Security Circular and the industry-developed guidelines, pipeline operators have been enhancing protective and deterrence measures. Measures include supplementing current emergency plans

with terrorist risk elements, strengthening physical barriers, tightening access controls, adjusting the frequency of patrols, and confirming response and recovery actions with local law enforcement and emergency officials. This program supports strategy 1.

TSA Smart Practices, Guidelines, Standards, Compliance, and Assessment Programs

Pipeline Security Smart Practices

The Pipeline Security Smart Practices reflect the application of data collected during the CSR process. This document is intended to assist the hazardous liquid and natural gas pipeline industries in their security planning and the implementation of security measures to protect their facilities, their assets, their people, and the public. This program supports strategies 1 and 4.

2002 DOT Pipeline Security Guidelines

Initially developed within DOT in conjunction with pipeline industry partners and adopted by TSA after its creation, these guidelines suggest minimum security levels for prevention, deterrence, and security incident response. Additionally, they provide a baseline and guidance for conducting assessments and determining criticality level. This program supports strategies 1 and 6.

Industry Smart Practices, Guidelines, Standards, Compliance, and Assessment Programs

AGA, Interstate Natural Gas Association of America, and American Public Gas Association, Security Guidelines: Natural Gas Industry, Transmission, and Distribution: Assessment Guidelines

Based on the 2002 DOT Pipeline Security Guidelines, these guidelines were issued in September 2002 and provide an approach for vulnerability assessment, critical facility definition, detection/deterrence methods, response and recovery, cyber security, and relevant operational standards for the natural gas industry. This program supports strategy 1.

Cryptographic Protection of Supervisory Control and Data Acquisition Communication (SCADA)

Developed primarily by AGA, these guidelines define a data encryption protocol method for securing SCADA systems against possible cyber security attacks. This program supports strategy 1.

American Petroleum Industry (API) Security in the Petroleum Industry: Practices Guidelines

These guidelines recommend security practices for all segments of the sector involving liquid and gas petroleum energy commodities. This program supports strategy 1.

API Pipeline SCADA Security Standard (API Standard 1164)

This API-developed guideline provides a model for proactive industry actions to improve the security of the Nation's energy infrastructure. This program supports strategy 1.

API Information Management and Technology Program

This API program provides a comprehensive review and quantitative assessment of company security programs, with focus on due care requirements, a database of security programs, and compliance initiatives. This program supports strategy 2.

Federal Grant Programs

Buffer Zone Protection Grants Program

This program is a DHS-sponsored grant program designed to provide resources to State, local, and tribal law enforcement officials to facilitate vulnerability identification and mitigation discussion between security partners and individual owners and operators. This program supports strategies 1 and 7.

Homeland
Security