Executive Summary

Transportation Security Environment

The Transportation Systems Sector—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 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.

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 appendixes establishes the Transportation Systems Sector'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:

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:

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 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 showed 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 sector's 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 the most 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[1]—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, 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

[1] 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.

evolving documents that should be updated annually to reflect the continuation of agreements, changes in legislation, or changes in the sector's security posture.