United States Government Accountability Office

GAO

Report to the Chairman, Committee on Homeland Security, House of Representatives

March 2009

# TRANSPORTATION SECURITY

## Comprehensive Risk Assessments and Stronger Internal Controls Needed to Help Inform TSA Resource Allocation

GAO
Accountability * Integrity * Reliability

# Highlights

Highlights of GAO-09-492, a report to the Chairman, Committee on Homeland Security, House of Representatives

## Why GAO Did This Study

The Department of Homeland Security (DHS) has called for using risk-informed approaches to help prioritize its investments, develop plans, and allocate resources in a way that balances security and commerce. Within DHS, the Transportation Security Administration (TSA) is responsible for making risk-informed investments to secure the transportation system. GAO evaluated to what extent TSA (1) implemented a risk management approach to inform the allocation of resources across the transportation sector and (2) followed internal control standards in its efforts to implement and use a risk management approach to inform resource allocation.

In conducting this work, GAO analyzed, among other things, DHS and TSA documents, such as TSA's risk management methodology, and compared them to DHS's risk management framework for infrastructure protection, compared TSA's management activities to criteria in federal internal control standards, and interviewed DHS and TSA officials.

## What GAO Recommends

To promote effective use of risk management, GAO is recommending, among other things, that the Assistant Secretary, TSA, work with DHS to validate its risk management approach, conduct comprehensive risk assessments, and establish related internal controls. DHS concurred with all of our recommendations.

View GAO-09-492 or key components.
For more information, contact Stephen M. Lord at (202) 512-4379 or lords@gao.gov.

March 2009

# TRANSPORTATION SECURITY

## Comprehensive Risk Assessments and Stronger Internal Controls Needed to Help Inform TSA Resource Allocation

## What GAO Found

TSA has taken some actions but has not fully implemented a risk management approach to inform the allocation of resources across the transportation modes (aviation, mass transit, highway, freight rail, and pipeline). DHS's risk management framework for infrastructure protection consists of six sequential steps that are used to systematically and comprehensively identify risk and establish risk-informed security priorities. TSA has taken some actions that the six steps require but has not conducted comprehensive risk assessments. For example, TSA collected information related to threat, vulnerability, and consequence within the transportation modes but has not conducted risk assessments that integrate these three components for each mode or the transportation sector as a whole. Identifying and prioritizing risk in this way is essential to efforts to allocate resources to address the highest priority risks. TSA developed an approach to prioritization based primarily on intelligence instead of comprehensive risk assessments. However, DHS has not reviewed or validated this methodology; thus, TSA lacks assurance that its approach provides the agency and DHS information needed to guide investment decisions to ensure resources are allocated to the highest risks. TSA also did not have a plan specifying the degree to which risk assessments are needed for the sector, the appropriate level of resources required to complete them, and time frames for completing its risk assessment efforts. Without a plan to identify the scope, resource requirements, and timeline for risk assessments, it will be difficult for TSA to ensure that it conducts timely and cost-effective risk assessments to inform resource allocation.

TSA has not followed federal internal control standards to assist it in implementing DHS's risk management framework and informing resource allocation. Specifically, TSA lacked the following:

- An organizational structure that allows the agency to direct and control operations to achieve agency objectives. Although TSA officials acknowledged that a focal point for TSA's risk management activities is needed, the agency has not yet established such a focal point.
- Policies, procedures, and guidance to assist its offices in ensuring that DHS's National Infrastructure Protection Plan (NIPP) risk management framework and related activities, such as risk assessments, are implemented as DHS and TSA intended for the transportation sector and its individual modes.
- A mechanism to monitor the quality of performance. While TSA reports to DHS on the implementation of its risk management activities, it did not discuss all of the steps necessary to implement DHS's risk management framework, such as the status of efforts taken to complete risk assessment activities including threat, vulnerability, and consequence assessments.

Without effectively implementing such controls, TSA cannot provide reasonable assurance that its resources are being used effectively and efficiently to achieve security priorities and that accountability and oversight regarding the quality of risk management activities implemented exists.

# Contents

**Tables**

# Figures

## Abbreviations

| | |
|---|---|
| ADASP | Aviation Direct Access Screening Program |
| ADRA | Air Domain Risk Assessment |
| BASE | Baseline Assessment and Security Enhancement |
| BDO | Behavior Detection Officer |
| CIKR | Critical Infrastructure and Key Resources |
| DHS | Department of Homeland Security |
| ERSC | Executive Risk Management Steering Committee |
| FAMS | Federal Air Marshals |
| FEMA | Federal Emergency Management Agency |
| FYHSP | Future Years Homeland Security Program |
| GCC | Government Coordinating Council |
| HSGP | Homeland Security Grant Program |
| HSPD-7 | Homeland Security Presidential Directive 7 |
| I&A | Office of Intelligence and Analysis |
| IP | Office of Infrastructure Protection |
| MANPADS | Man-Portable Air Defense Systems |
| MSRAM | Maritime Security Risk Analysis Model |
| NIPP | National Infrastructure Protection Plan |
| NTSRA | National Transportation Sector Risk Analysis |
| OI | Office of Intelligence |
| OMB | Office of Management and Budget |
| OMRR | Objectively Measured Risk Reduction |
| PPBE | Planning, Programming, Budgeting, and Execution |
| RAP | Resource Allocation Plan |
| RMA | Office of Risk Management and Analysis |
| RMSI | Office of Risk Management and Strategic Innovation |
| SAAP | Security Analysis and Action Program |
| SBRM | Systems-Based Risk Management |
| SCC | Sector Coordinating Council |
| SHIRA | Strategic Homeland Infrastructure Risk Assessment |
| TSA | Transportation Security Administration |
| TSNM | Office of Transportation Sector Network Management |
| TS-SSP | Transportation Systems Sector-Specific Plan |
| VIPR | Visible Intermodal Prevention and Response |

GAO
Accountability * Integrity * Reliability

**United States Government Accountability Office**
**Washington, DC 20548**

March 27, 2009

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
House of Representatives

Dear Mr. Chairman:

Recent terrorist events have demonstrated that transportation systems remain targets of attack worldwide. The July 2006 rail attacks in Mumbai, India, and the alleged August 2006 terrorist plot to detonate liquid explosives onboard multiple commercial aircraft bound for the United States from the United Kingdom underscore the vulnerability of transportation systems worldwide to terrorist attack and highlight the need to focus on the security of these systems. Securing this transportation system is an enormously complicated undertaking. In the United States, the nation's transportation system includes roughly 4 million miles of roads and highways, more than 100,000 miles of rail, 600,000 bridges, more than 300 tunnels, numerous sea ports, 2 million miles of pipeline, 500,000 train stations, and 500 public-use airports.[1] Key modes of transportation include aviation, freight rail, highway, maritime, mass transit, and pipeline. The transportation system crisscrosses the nation and extends beyond our borders to move millions of passengers and tons of freight each day. Securing the system is further complicated by the number of private and public stakeholders involved in operating and protecting the system and the need to balance security with the expeditious flow of people and goods.

The Department of Homeland Security's (DHS) mission includes preventing terrorist attacks, reducing vulnerabilities, minimizing damages from attacks, and aiding recovery efforts. Within DHS, the Transportation Security Administration (TSA) is responsible for securing the transportation system while facilitating commerce and ensuring the freedom of movement for the traveling public. Since it is not practical or feasible to protect all assets and systems against every possible terrorist threat, DHS has called for using risk-informed approaches to prioritize its

[1] Department of Homeland Security, Transportation Security Administration, Transportation Systems Sector-Specific Plan, May 2007.

investments and for developing plans and allocating resources in a way that balances security and commerce.[2] A risk management approach entails a continuous process of managing risk through a series of actions, including setting strategic goals and objectives, assessing risk, evaluating alternatives, selecting initiatives to undertake, and implementing and monitoring those initiatives. In June 2006, DHS issued the National Infrastructure Protection Plan (NIPP), which named TSA as the primary federal agency responsible for coordinating critical infrastructure protection efforts within the transportation sector.[3] The NIPP also established a six-step risk management framework to establish national priorities, goals, and requirements for Critical Infrastructure and Key Resources (CIKR) protection so that federal funding and resources are applied in the most effective manner to deter threats, reduce vulnerabilities, and minimize the consequences of attacks and other incidents.[4] The NIPP defines risk as a function of threat, vulnerability, and consequence. Threat is an indication of the likelihood that a specific type of attack will be initiated against a specific target or class of targets. Vulnerability is the probability that a particular attempted attack will succeed against a particular target or class of targets. Consequence is the effect of a successful attack.

Our past work examining TSA found that it has undertaken numerous initiatives to strengthen transportation security, particularly in aviation. However, we also reported that TSA could strengthen its risk-informed efforts to include conducting systematic analysis to prioritize its security

[2] Risk-based decision making has often been used interchangeably with risk-informed decision making. However, according to the DHS Risk Lexicon, risk-based decision making uses the assessment of risk as the primary decision driver, while risk-informed decision making may consider other relevant factors in addition to risk information. In keeping with this distinction, we have used the term risk-informed rather than risk-based throughout this report.

[3] Issued in December 2003, Homeland Security Presidential Directive 7 (HSPD-7) directed the Departments of Transportation and Homeland Security to collaborate on all matters relating to transportation security and transportation infrastructure protection. DHS subsequently designated TSA as the lead agency for addressing HSPD-7 as it relates to securing the nation's transportation sector.

[4] CIKR include the assets, systems, networks, and functions that provide vital services to the nation and are dispersed among the following 18 sectors: Agriculture and Food; Banking and Finance; Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Government Facilities; Healthcare and Public Health; Information Technology; National Monuments and Icons; Nuclear Reactors, Materials, and Waste; Postal and Shipping; Transportation Systems; and Water.

investments.[5] Although TSA has implemented risk-informed efforts with many of its programs and initiatives, we reported that—because of circumstances beyond TSA's control and a lack of planning—TSA has not always conducted the systematic analysis needed to inform its decision-making processes and to prioritize investments in security programs. For example, we reported that TSA has not always conducted needed assessments of threats, vulnerabilities, and consequences to inform the allocation of its resources and has not fully assessed alternatives that could be pursued to achieve efficiencies and potentially enhance security.

You asked us to evaluate the extent to which TSA has implemented a risk-informed framework to guide federal programs and responses to better prepare against terrorism and other threats and to better direct finite resources to the areas of highest priority. This report answers the following questions: (1) to what extent has TSA implemented a risk management approach consistent with the NIPP to inform the allocation of resources across the transportation sector and (2) to what extent has TSA followed internal control standards in its efforts to implement a risk management approach and use it to inform resource allocation.

This report is a public version of a restricted report (GAO-09-319SU) that we are providing to you concurrently. DHS and TSA deemed some of the information in the restricted report to be sensitive security information, which must be protected from public disclosure. Although this report omits that information, such as specific details associated with hypothetical terrorist threat scenarios, it addresses the same questions as the restricted report. Also, the overall methodology used for both reports is the same.

To assess the extent to which TSA has made progress in implementing a risk management approach to inform the allocation of resources across the transportation sector, we analyzed DHS and TSA internal documents, such as agency memoranda, TSA's risk management methodology and the Transportation Systems Sector-Specific Plan and its modal annexes, and

[5] See GAO, *Transportation Security: Systematic Planning Needed to Optimize Resources*, GAO-05-357T (Washington, D.C. June 29, 2005); *Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts*, GAO-07-225T (Washington, D.C.: Jan. 18, 2007); *Commercial Vehicle Security: Risk-Based Approach Needed to Secure the Commercial Vehicle Sector*, GAO-09-85 (Washington, D.C.: Feb. 6, 2009); and *Highway Infrastructure: Federal Efforts to Strengthen Security Should Be Better Coordinated and Targeted on the Nation's Most Critical Highway Infrastructure*, GAO-09-57 (Washington, D.C.: Jan. 30, 2009).

compared them to criteria in the NIPP's risk management framework. We also reviewed relevant laws; presidential directives; budget procedures, priorities, and submissions; TSA management directives; and our prior work on risk management and transportation security. We analyzed DHS budgeting and planning guidance, such as the resource allocation plan and sector annual report instructions, to determine the extent to which risk management was to inform TSA practices. Further, we interviewed DHS and TSA officials to identify TSA's risk management efforts at the strategic and modal levels and the extent to which TSA had implemented the NIPP's risk management framework. We also interviewed DHS and TSA officials to identify alignment between the allocation of resources and stated priorities. In conducting this work, we limited our analysis to the five modes of the transportation sector that TSA is responsible for securing: aviation, freight rail, highway infrastructure and motor carrier, mass transit, and pipeline.[6] Further, while the private sector, state, local, and tribal governments, and other federal agencies have roles in securing the transportation sector, we limited our analysis to activities conducted by TSA. Due to the scope of our work, we relied on TSA to identify its assessment activities but did not assess the extent to which its assessment activities meet the NIPP criteria for threat, vulnerability, and consequence assessments.

To identify the extent to which TSA has followed internal control standards in its efforts to implement a risk management approach and use it to inform resource allocation, we compared controls TSA designed to assist in its risk management efforts with criteria in standards for internal control in the federal government.[7] Specifically, we focused on the extent to which TSA established a focal point; clearly defined roles and responsibilities; set policies, procedures, and guidance; and created a monitoring system for implementing a risk management framework. We also reviewed our past reports on risk management and transportation

[6] We did not include the maritime mode of transportation in our analysis because the United States Coast Guard is the primary agency responsible for maritime security.

[7] See GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: Nov. 1999). These standards, issued pursuant to the requirements of the Federal Managers' Financial Integrity Act of 1982, provide the overall framework for establishing and maintaining internal control in the federal government. Also pursuant to the 1982 Act, the Office of Management and Budget (OMB) issued circular A-123, revised December 21, 2004, to provide the specific requirements for assessing the reporting on internal controls. Internal control standards and the definition of internal control in OMB Circular A-123 are based on GAO's *Standards for Internal Control in the Federal Government.*

security and documentation provided by DHS and TSA on the organization of TSA's risk management office and its monitoring system. We conducted interviews with DHS and TSA officials to identify their internal controls. In our interviews, we asked DHS and TSA officials to identify any factors that affected implementation of the risk management framework and its use to inform resource allocation.

We conducted this performance audit from February 2008 through March 2009 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

# Background

## Legislation and Presidential Directives Require the Development of a Risk Management Approach for the Transportation Sector

In recent years, the President and Congress have provided that federal agencies with homeland security responsibilities are to apply risk management principles to inform their decision making regarding allocating limited resources and prioritizing security activities.[8] They have done this through Homeland Security Presidential Directives (HSPD)[9] and laws, such as the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act) and the Intelligence Reform and

[8] See The National Strategy for Homeland Security, October 2007: "Despite our best efforts, achieving a complete state of CIKR protection is not possible in the face of the numerous and varied catastrophic possibilities that could challenge the security of America today. Recognizing that the future is uncertain and that we cannot envision or prepare for every potential threat, we must understand and accept a certain level of risk as a permanent condition…The assessment and management of risk underlies the full spectrum of our homeland security activities, including decisions about when, where, and how to invest in resources that eliminate, control, or mitigate risks."

[9] See, e.g., Homeland Security Presidential Directive/HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection (Dec. 17, 2003).

Terrorism Prevention Act of 2004.[10] The Homeland Security Act of 2002, which established DHS, also directed the department's former Directorate of Information Analysis and Infrastructure Protection to use risk management principles in coordinating the nation's critical infrastructure protection efforts.[11] This requirement includes integrating relevant information, analysis, and vulnerability assessments to identify priorities for protective and support measures by the department, other federal agencies, state and local government agencies and authorities, the private sector, and other entities. Homeland Security Presidential Directive 7 (HSPD-7) and the Intelligence Reform and Terrorism Prevention Act further define and establish critical infrastructure protection responsibilities for DHS and Sector-Specific Agencies, which are federal departments and agencies responsible for Critical Infrastructure and Key Resources (CIKR) protection activities in specified CIKR sectors such as transportation. In particular, HSPD-7 required the development of a comprehensive, integrated national plan for CIKR protection, the NIPP, which in turn required the development of a Transportation Systems Sector-Specific Plan (TS-SSP). Table 1 shows the relationship and responsibilities established by HSPD-7, the NIPP, and the TS-SSP.[12]

[10] See, e.g., Pub. L. No. 110-53, § 1202, 121 Stat. 266, 381-83 (2007) (amending 49 U.S.C. § 114(s), as redesignated); Pub. L. No. 108-458, § 4001, 118 Stat. 3639, 1370, 3710-12 (2004) (codifying 49 U.S.C. § 114(s), as redesignated, and amending 49 U.S.C. § 44904). In general, section 114(s), as codified and amended, requires the Secretary of Homeland Security to develop, prepare, implement, and update a National Strategy for Transportation Security and modal security plans that address security risks, including threats, vulnerabilities, and consequences.

[11] See Pub. L. No. 107-296, § 201, 116 Stat. 2135, 2145-49 (2002). In 2006, DHS reorganized its Directorate of Information Analysis and Infrastructure Protection. The functions of the Directorate of Information Analysis and Infrastructure Protection were moved to the Office of Intelligence and Analysis and Office of Infrastructure Protection.

[12] TSA's Transportation Systems Sector-Specific Plan describes a risk management framework known as the Systems-Based Risk Management (SBRM) Framework (see app. I for a description).

**Table 1: Risk Management in Transportation Sector Key Documents**

| | | |
|---|---|---|
| Presidential level | **HSPD-7**<br>Homeland Security Presidential Directive<br>*December 2003* | HSPD-7 required DHS to produce a comprehensive, integrated national plan for CIKR protection, and DHS designated TSA as the sector-specific agency in charge of the transportation sector |
| Department level<br>**DHS** | **NIPP**<br>National Infrastructure Protection Plan<br>*June 2006* | DHS issued the NIPP which required TSA and other sector-specific agencies to support and align with the NIPP risk management framework |
| Component level<br>**TSA** | **TS-SSP**<br>Transportation Systems Sector-Specific Plan<br>*May 2007* | TSA developed the TS-SSP to comply with NIPP requirements which detailed a strategic risk management framework for the sector that aligned with NIPP guidance |

Sources: GAO presentation of DHS and TSA information.

DHS's 2008 Strategic Plan also identifies risk management as an important tool for decision making. The plan states that securing the country from every conceivable threat is not feasible, and consequently, the department has instituted risk management as the primary basis for policy and resource allocation decisions. The plan explains that in the government's complex and resource-constrained environment, DHS will use quantitative and qualitative risk assessments to help guide resource decisions. Effective risk assessments will allow these resources to target the most significant threats, vulnerabilities, and potential consequences and will provide assurances that priorities and investments are based on the best information available.

## GAO and DHS Have Developed Similar Risk Management Frameworks

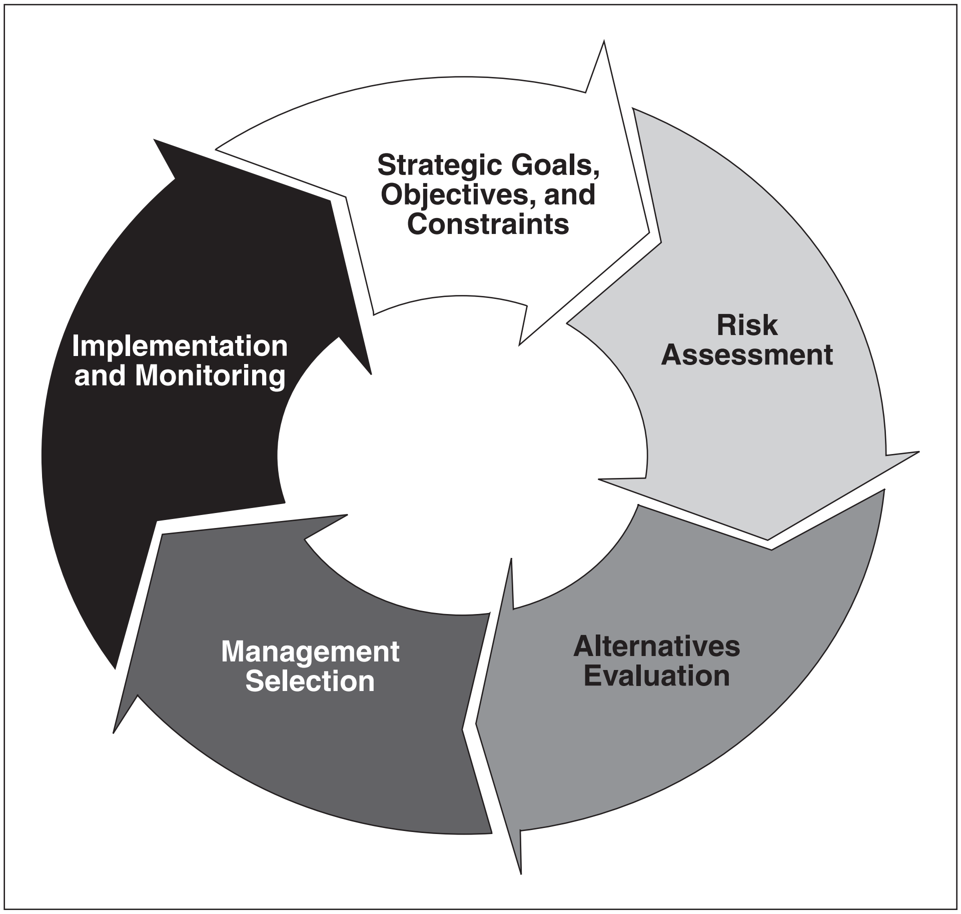
Risk management is a tool for informing policymakers' decisions about assessing risks, allocating resources, and taking actions under conditions of uncertainty. We have previously reported that a risk management approach can help to prioritize and focus the programs designed to combat terrorism.[13] Risk management, as applied in the transportation security context, can help federal decision makers determine where and how to invest limited resources within and among the various modes of transportation.

To provide guidance to agency decision makers, we developed a risk management framework which is intended to be a starting point for applying risk-informed principles.[14] Our risk management framework, shown in figure 1, entails a continuous process of managing risk through a series of actions, including setting strategic goals and objectives, assessing risk, evaluating alternatives, selecting initiatives to undertake, and implementing and monitoring those initiatives.

[13] See, for example, GAO, *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*, GAO-06-91 (Washington, D.C.: Dec. 15, 2005); GAO-07-255T; *Department of Homeland Security: Progress Report on Implementation of Mission and Management Functions*, GAO-07-454 (Washington, D.C.: Aug. 17, 2007); and *Risk Management: Strengthening the Use of Risk Management Principles in Homeland Security*, GAO-08-904T (Washington, D.C.: June 25, 2008).

[14] See GAO 06-91.

Figure 1: GAO Risk Management Framework


Strategic Goals, Objectives, and Constraints
Risk Assessment
Alternatives Evaluation
Management Selection
Implementation and Monitoring

Source: GAO.

Setting strategic goals, objectives, and constraints is a key first step in applying risk management principles and helps to ensure that management decisions are focused on achieving a purpose. These decisions should take place in the context of an agency's strategic plan that includes goals and objectives that are clear and concise. The ability to achieve strategic goals depends, in part, on how well an agency manages risk. The agency's strategic plan should address risk-related issues that are central to the agency's overall mission.

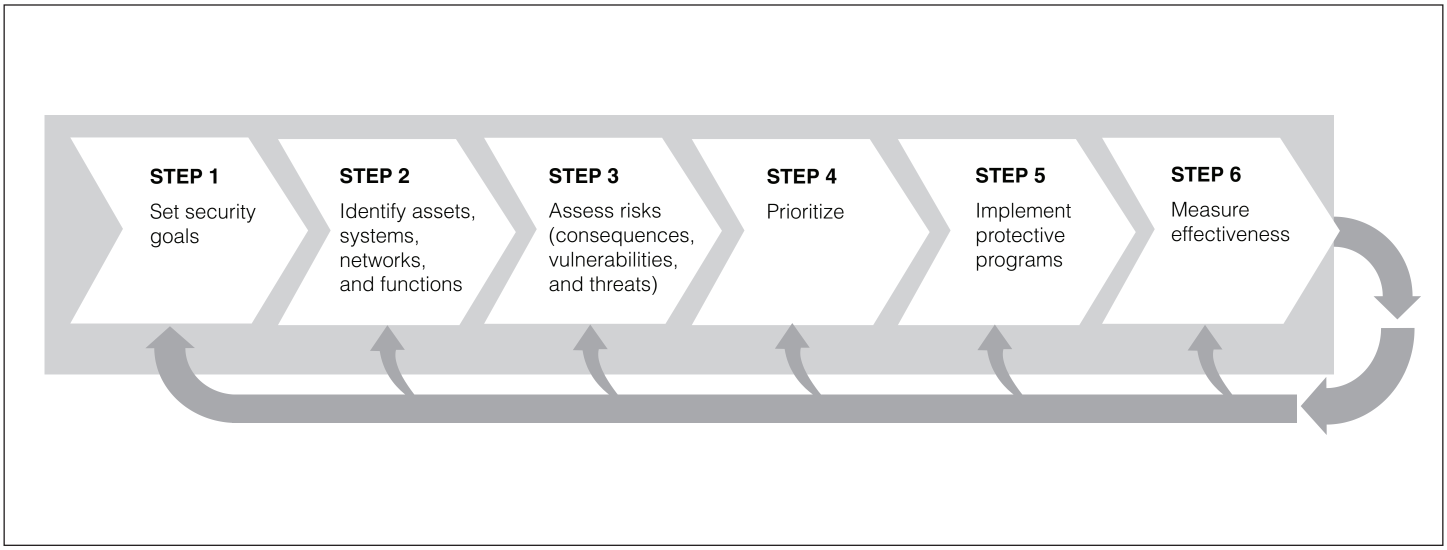
Risk assessment, an important element of a risk-informed approach, helps decision makers identify and evaluate potential risks so that countermeasures can be designed and implemented to prevent or mitigate the effects of the risks. Risk assessment is a qualitative and/or quantitative determination of the likelihood of an adverse event occurring and the severity, or impact, of its consequences. Risk assessment in a homeland security application involves assessing three key components—threat, vulnerability, and consequence. A threat assessment is the identification and evaluation of adverse events that can harm or damage an asset. A vulnerability assessment identifies weaknesses in physical structures, personal protection systems, processes, or other areas that may be exploited. A consequence assessment is the process of identifying or evaluating the potential or actual effects of an event, incident, or occurrence. Information from these three assessments contributes to an overall risk assessment that characterizes risks, for example, rating them on a scale of high, medium, or low. Such information provides input for evaluating alternatives and prioritizing security initiatives. The risk assessment element in the overall risk management cycle informs each of the remaining steps of the cycle.

Alternatives evaluation addresses the evaluation of risk reduction methods by consideration of countermeasures or countermeasure systems and the costs and benefits associated with them. Management selection addresses such issues as determining where resources and investments will be made, the sources and types of resources needed, and where those resources would be targeted. Finally, implementation and monitoring address the degree to which risk management strategies contain internal controls and performance measurement guidelines. In addition to implementing countermeasures, it may also include implementing new organizational policies and procedures, as well as human, physical, and technical controls.

The 2006 NIPP, issued by DHS, included a risk management framework. This framework consists of six steps (see fig. 2), which for the most part mirror GAO's risk management framework.[15]

[15] The six-step risk management framework described by DHS in the National Infrastructure Protection Plan is consistent with GAO's five-step risk management framework described in GAO-06-91. While the content and sequence of the frameworks is effectively the same, the frameworks differ in the number of steps and the degree to which actions are divided or combined into different steps. For example, the second step in the GAO framework (Risk Assessment) is separated into the second and third steps in the NIPP framework (Identify Assets and Systems, and Assess Risks, respectively). DHS also recently issued an Interim Integrated Risk Management Framework for DHS-wide risk management purposes that is similar, differing only in the subdivision of the steps.

Figure 2: NIPP Risk Management Framework


STEP 1
Set security goals
STEP 2
Identify assets, systems, networks, and functions
STEP 3
Assess risks (consequences, vulnerabilities, and threats)
STEP 4
Prioritize
STEP 5
Implement protective programs
STEP 6
Measure effectiveness

Sources: GAO presentation of DHS information.

(1) Set security goals: Define specific outcomes, conditions, end points, or performance targets that collectively constitute an effective protective posture.

(2) Identify assets, systems, networks, and functions: Develop an inventory of the assets, systems, and networks that comprise the nation's critical infrastructure, key resources, and critical functions. Collect information pertinent to risk management that takes into account the fundamental characteristics of each sector.

(3) Assess risks: Determine risk by combining general or specific threat information, known vulnerabilities to various potential attack vectors, potential direct and indirect consequences of a terrorist attack or other hazards (including seasonal changes in consequences, and dependencies and interdependencies associated with each identified asset, system, or network).

(4) Prioritize: Aggregate and analyze risk assessment results to develop a comprehensive picture of asset, system, and network risk; establish priorities informed by risk; and determine protection and business continuity initiatives that provide the greatest mitigation of risk.

(5) Implement protective programs: Select sector-appropriate protective actions or programs to reduce or manage the risk identified and secure the resources needed to address priorities.

(6) Measure effectiveness: Use metrics and other evaluation procedures at the national and sector levels to measure progress and assess the effectiveness of the national CIKR protection program in improving protection, managing risk, and increasing resiliency.

Like GAO's framework, the NIPP's risk management framework is a repetitive process that continuously uses the results of each step to inform the activities in both subsequent and previous steps over time. The six steps of the NIPP risk management framework are designed to produce a systematic and comprehensive understanding of risk and ultimately provide for security investments based on this knowledge of risk. In February 2009, DHS revised and reissued the NIPP. The six-step risk management framework remains unchanged.

## TSA Has Not Fully Implemented the Risk Management Framework Required by the NIPP to Inform Resource Allocation across the Transportation Sector

TSA has not fully implemented the risk management framework required by the NIPP to inform the allocation of resources across the transportation sector. While TSA has taken some actions to complete the six steps required by the NIPP framework, it has not conducted comprehensive risk assessments, a key step needed to complete the other steps required by the framework. Conducting comprehensive risk assessments as envisioned by the NIPP would improve TSA's evaluation of risk for the transportation sector and its individual modes and help improve its efforts to allocate resources to those areas with the highest priority risks. Instead of conducting comprehensive risk assessments, TSA has used an intelligence-driven approach to risk management. Officials cited high costs and methodological difficulties as reasons for taking this approach rather than fully implementing the NIPP framework.

## TSA Took Action to Implement the NIPP's Six-Step Risk Management Framework but Could Strengthen Efforts by Conducting Comprehensive Risk Assessments, a Key Step

TSA has taken action to implement the first two steps of the NIPP's risk management framework, but has not conducted comprehensive risk assessments, the third step, which is key in conducting the remaining three steps of the six-step framework. TSA developed security goals, in accordance with the NIPP's first step, but did not approve or circulate them. Further, TSA established a database to track assets and systems, the second step of the NIPP. However, while TSA's assessments contain elements of risk—threat, vulnerability, and consequence—TSA does not combine these elements to estimate risk for each transportation mode. Without comprehensive risk assessments, TSA cannot ensure that its priorities, protective programs, and measurements of effectiveness are risk-informed, steps four through six of the NIPP.

### TSA has Taken Some Actions to Set Security Goals and Identify Assets, Systems, Networks, and Functions

Setting security goals is the first step in the NIPP framework. TSA developed and published the following goals in its May 2007 Transportation Systems Sector-Specific Plan (TS-SSP):

(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.

However, TSA did not define specific outcomes, conditions, end points, or performance targets for these goals as called for by the NIPP. The TS-SSP also calls for the establishment of specific security goals, which TSA developed but did not approve or circulate.[16] These goals were not approved or circulated because they were part of a discontinued risk management effort (see app. I for details on this effort). According to TSA, these specific goals were to represent TSA's highest risk mitigation priorities, expressed as high level consequences to be prevented or otherwise mitigated, and would establish specific, measurable, realistic, attainable targets that, when achieved, were to reduce the risk to the sector. Unless TSA approves and circulates specific goals, it will be difficult for TSA to prioritize what risks to assess, what countermeasures to deploy, and what performance to measure.

TSA has taken actions to identify assets and systems, the second step of the NIPP. DHS, through its Office of Infrastructure Protection (IP),

[16] DHS determined that details on the specific security goals are sensitive security information. Details on the goals are provided in the restricted version of this report, GAO-09-319SU.

established an Infrastructure Data Warehouse, which includes infrastructure data from a variety of federal, state, and local sources and other authoritative open source infrastructure databases. TSA has updated the transportation source data and worked with DHS to expand the database. TSA has also worked with DHS's Homeland Infrastructure Threat and Risk Analysis Center to identify and prioritize assets that, according to DHS, if destroyed, damaged, or otherwise compromised, could create very significant consequences on a regional or national scale. According to DHS, this prioritized critical infrastructure list provides a common basis for DHS and its security partners to plan and undertake CIKR protective efforts.[17]

## TSA Has Taken Some Actions but Has Not Conducted Comprehensive Risk Assessments for the Transportation Sector

To be considered credible, the NIPP states that a risk assessment must specifically address the three components of risk: threat, vulnerability, and consequence. The NIPP also states that after these three components have been assessed, they are to be combined to provide an estimate of the expected loss considering the likelihood of an attack or other incident. Further, to be not only credible but comparable to other methodologies, according to the NIPP's criteria, risk assessments must be documented, transparent (to avoid bias in assumptions), reproducible (so that other experts can verify the results), and accurate. Comprehensive risk assessments must have these qualities so that they can be used to support comparisons of risk, planning, and resource prioritization at the national level. In December 2005, we reported that a lack of information that fully depicts threats, vulnerabilities, and consequences limits an organization's ability to establish priorities and make cost-effective countermeasure decisions.[18]

TSA had not conducted comprehensive risk assessments in a manner consistent with the NIPP criteria. In 2007, TSA initiated but later discontinued an effort to conduct a comprehensive risk assessment for the entire transportation sector, known as the National Transportation Sector Risk Analysis (NTSRA). Specifically, TSA was planning to estimate the threat, vulnerability, and consequence of a range of hypothetical attack scenarios and integrate these estimates to produce risk scores for each scenario that could be compared among each of the modes of

[17] DHS determined that details on the prioritized critical infrastructure list are sensitive security information. Details on this list are provided in the restricted version of this report, GAO-09-319SU.

[18] See GAO-06-91.

transportation.[19,20] However, TSA discontinued its work on the NTSRA because officials stated that estimating the likelihood of terrorist threats was difficult to quantify.[21]

Further, although TSA reported that it conducted assessments within each mode of transportation to gather information related to threat, vulnerability, and consequence, it has not integrated this information into comprehensive, credible risk assessments that meet the NIPP criteria. Table 2 provides an overview of assessment activities TSA reported having conducted (see app. II for details on these activities).[22]

[19] TSA intended NTSRA to address GAO, congressional, and other concerns that TSA had not conducted a comprehensive risk assessment for the transportation sector. As part of its initial efforts, TSA identified 38 distinct threat scenarios for the transportation sector as part of NTSRA—including a variety of conventional explosive attacks as well as chemical and biological attacks—but it did not produce a risk score for these scenarios by integrating threat, vulnerability, and consequence assessments.

[20] DHS determined that details on the 38 NTSRA threat scenarios are sensitive security information. Details on these scenarios are provided in the restricted version of this report, GAO-09-319SU.

[21] As a result, in July 2008, TSA stated that progress on NTSRA had been suspended, and in September 2008, TSA stated that NTSRA would not be issued or used. However, in December 2008 TSA stated that it was developing a Risk Management Executive Steering Committee that would reconsider the status of NTSRA.

[22] Due to the scope of our work, we did not assess the extent to which these assessment activities meet the NIPP criteria for threat, vulnerability, and consequence assessments.

Table 2: Summary of TSA's Current Assessment Activities

| | | Risk information provided | | | Risk assessment conducted (including threat, vulnerability, and consequence)[a] |
|---|---|---|---|---|---|
| Mode | Program activity title | Threat | Vulnerability | Consequence | |
| Multiple modes | Administrators Daily Intelligence Briefing | Yes | No | No | No |
| | Homeland Information Report | Yes | No | No | |
| | Note to Administrator | Yes | No | No | |
| | Strategic Homeland Infrastructure Risk Assessment | No | Yes | Yes | |
| | Spot Reports | Yes | No | No | |
| | Special Event Threat Assessments | Yes | No | No | |
| | Transportation Intelligence Gazettes | Yes | No | No | |
| | Transportation Suspicious Incidents Report | Yes | No | No | |
| Aviation | Air Cargo Vulnerability Assessments | No | Yes | No | No |
| | Aviation Mode Annual Threat Assessment | Yes | No | No | |
| | Current Airport Threat Assessment | Yes | No | No | |
| | Joint Vulnerability Assessments | No | Yes | No | |
| | Man-Portable Air Defense Systems (MANPADS) Vulnerability Assessments | No | Yes | No | |
| | No-Fly/Selectee Lists | Yes | No | No | |
| Freight rail | Corporate Security Reviews | No | Yes | No | No |
| | Freight Rail Mode Annual Threat Assessment | Yes | No | No | |
| | Rail Corridor Reviews | No | Yes | Yes | |
| | Toxic Inhalation Hazard (TIH) Rail Risk Monitoring Program | No | Yes | Yes | |
| Highway infrastructure and motor carrier | Corporate Security Reviews | No | Yes | No | No |
| | Highway Infrastructure and Motor Carrier Mode Annual Threat Assessment | Yes | No | No | |
| Mass transit | Baseline Assessment and Security Enhancement review (BASE) | No | Yes | No | No |
| | Mass Transit Mode Annual Threat Assessment | Yes | No | No | |
| | Security Analysis and Action Program (SAAP) | No | Yes | No | |

| | | Risk information provided | | | Risk assessment conducted (including threat, vulnerability, and consequence)[a] |
|---|---|---|---|---|---|
| **Mode** | **Program activity title** | **Threat** | **Vulnerability** | **Consequence** | |
| **Pipeline** | Acute Assessment | Yes | No | No | No |
| | Corporate Security Reviews | No | Yes | No | |
| | Pipeline Cross-Border Vulnerability Assessments Program | No | Yes | No | |
| | Pipeline Mode Annual Threat Assessment | Yes | No | No | |

Sources: TSA and GAO analysis.

[a] A risk assessment requires a combination of all three components of risk, and in these cases no efforts were made to combine the components into a comprehensive risk assessment.

As table 2 shows, while TSA reported that it conducted assessments related to individual components of risk for certain modes of transportation, risk assessments providing quantitative analysis that combine the three components of risk had not been conducted for any mode. Examples of TSA's assessment activities include the following:

- TSA's Office of Intelligence produces an annual threat assessment for the aviation mode, among other intelligence products. These assessments provide information on individuals who could carry out attacks, tactics they might use, and potential targets. TSA's most recent aviation threat assessment, dated December 2008, identifies that terrorists worldwide continue to view civil aviation as a viable target for attack and as a weapon that can be used to inflict mass casualties and economic damage. It also concluded that improvised explosive devises and hijackings pose the most dangerous terrorist threat to commercial airliners in the United States.

- Consistent with direction specified in law,[23] and partly in response to our recommendations, TSA implemented an Air Cargo Vulnerability Assessment Program in November 2006. In August 2008, we reported that TSA officials stated that the agency had conducted air cargo

[23] See Pub. L. No. 110-28, 121 Stat. 112, 140-41 (2007) (providing that the $80 million appropriated for air cargo shall be used to complete air cargo vulnerability assessments for all Category X airports, among other purposes). TSA classifies the commercial airports in the United States into one of five security risk categories (X, I, II, III, and IV). In general, Category X airports have the largest number of passenger boardings, and category IV airports have the smallest. Category X, I, II, and III airports account for more than 90 percent of the nation's air traffic.

vulnerability assessments at six domestic airports and planned to conduct air cargo vulnerability assessments at all 27 domestic Category X airports by the end of calendar year 2009.

- As we reported in January 2009, in the highway infrastructure and motor carrier mode, TSA conducts annual threat assessments, as well as corporate security reviews—a type of assessment related to vulnerability information.[24] For highway infrastructure, these corporate security reviews largely consist of interviews with state officials to assess the security plan, policies, and security actions of organizations whose operations include critical highway infrastructure. According to highway motor carrier officials, the goal of these reviews is to evaluate potential security gaps and provide suggested actions to state officials for strengthening them.

According to TSA, in addition to its current assessment activities, it is planning to conduct assessments required by the 9/11 Commission Act on railroad transportation, school buses,[25] rail tank cars, and general aviation airports. Although TSA did not follow the NIPP's approach to assessing risk, TSA officials stated that a high-risk focus is determined for each mode.[26] While TSA's efforts may provide useful information, TSA's approach to assessing vulnerability and consequence is not based on the NIPP's criteria. Doing so is important to providing reasonable assurances

[24] See GAO-09-57.

[25] In addition to the 9/11 Commission Act requirement for a school bus risk assessment, TSA reports that it plans to conduct risk assessments for the other major components of the highway system: truck, over-the-road bus, commercial trucking and port interface, and highway infrastructure.

[26] According to TSA, the high-risk focus for a mode is informed by intelligence insights; vulnerability studies such as corridor assessments in rail; scientific analysis such as a study conducted by the Homeland Security Institute for general aviation; proxies for consequence such as ridership and the number of underground tunnels in mass transit; security incidents at airports; 9/11 Commission Act requirements such as 100 percent screening of cargo transported on passenger aircraft; and other relevant information. As a result, TSA's approach to identifying high-risk focus areas is not based on criteria in the NIPP. For example, TSA stated that transportation system partners and owners and operators provide input into vulnerability analysis, rather than follow NIPP guidance that would have TSA identify consistent methodologies and tools for transportation assets and systems and then identify and group vulnerabilities using common threat scenarios. Further, TSA stated that consequences are typically assessed using historic analogs—roughly similar events for which the consequences have been observed—rather than an assessment of the effects of such an attack on people, the economy, public confidence, and the government's capability, as required by the NIPP.

that TSA's resources have been allocated to programs designed to protect assets that face relatively higher risk.

Although TSA has not conducted comprehensive risk assessments as required by the NIPP, TSA participates in DHS's effort to assess risk across and within each of the nation's 18 CIKR sectors. DHS's effort is documented in an annual, classified product, known as the Strategic Homeland Infrastructure Risk Assessment (SHIRA). According to DHS, the White House is the principal consumer of SHIRA information. To develop SHIRA, DHS works with members of the Intelligence Community to determine applicable threats against various systems and assets. TSA then estimates vulnerabilities and consequences resulting from scenarios involving these threats by providing scores, based on professional judgment, and enters these data onto a worksheet which TSA certifies as the official record of its position and participation in SHIRA. However, TSA does not combine this threat, vulnerability, and consequence information to develop a comprehensive risk assessment, nor does TSA use this information to set agency goals or inform its resource allocation process.

As we reported in January 2009, other federal agencies have conducted assessments that could be useful to TSA in considering how to design and complete risk assessments, but TSA has not leveraged these assessments.[27] For example, federal entities have collectively conducted asset-level vulnerability assessments on a substantial percentage of highway infrastructure assets identified on the 2007 prioritized critical infrastructure list.[28] However, limited mechanisms exist to share the assessment results among the various federal partners to inform their own assessment efforts. For example, TSA's Highway Motor Carrier Division reported that it is generally unfamiliar with the assessment processes, mechanisms, and results of the other DHS entities, particularly the Office of Infrastructure Protection (IP). Lacking adequate coordination mechanisms, the potential for duplication and inadequate leveraging of federal resources exists.[29] For example, multiple vulnerability assessments

[27] See GAO-09-57.

[28] DHS determined that details on the prioritized critical infrastructure list are sensitive security information. Details on this list are provided in the restricted version of this report, GAO-09-319SU.

[29] According to DHS, the Office of Risk Management and Analysis (RMA) has recognized this as an issue internal to DHS, and will require components to share results with RMA.

were conducted by federal agencies for numerous assets that were on the fiscal year 2007 prioritized critical infrastructure list.[30] Specifically, IP and the U.S. Coast Guard conducted assessments on a number of the same assets identified as critical. Given the number of highway infrastructure assets identified as critical, it is especially important to ensure that future risk assessment efforts are effectively coordinated between federal entities and the results shared among these entities. For this reason, we recommended that TSA incorporate the results of available threat, vulnerability, and consequence information into the strategy for securing highway infrastructure.[31] DHS and TSA agreed with our recommendation, and TSA is working to address it.

## Conducting Comprehensive Risk Assessments Would Allow TSA to Provide Reasonable Assurances That Its Priorities, Protective Programs, and Measurements of Effectiveness are Risk-Informed

TSA has taken actions to set priorities, the fourth step of the NIPP, but without comprehensive risk assessments it is difficult to prioritize what risks to address and to what degree. The NIPP states that security partners should establish priorities based on risk analysis that, consistent with NIPP criteria, combine threat, vulnerability, and consequence assessments. The NIPP further states that an estimate of the benefits resulting from actions taken to mitigate risk must be combined with estimates of their costs in a cost-benefit analysis to prioritize and choose among various protective measures. TSA has identified three priorities in its CIKR sector annual report:[32]

(1) Protect the nation's transportation systems from attacks involving explosives,
(2) Manage and reduce the risk associated with key nodes, links, and flows within critical transportation systems to improve overall network survivability,
(3) Align sector resources with the highest priority transportation risks using risk analysis and economic analysis as decision criteria.

[30] DHS determined that details on the prioritized critical infrastructure list are sensitive security information. Details on this list are provided in the restricted version of this report, GAO-09-319SU.

[31] See GAO-09-57.

[32] HSPD-7 requires Sector-Specific Agencies to provide an annual report to the Secretary of Homeland Security on their efforts to identify, prioritize, and coordinate CIKR protection in their respective sectors. Consistent with this requirement, DHS provides reporting guidance and templates that include requests for specific information, such as sector CIKR protection priorities, requirements, and resources. TSA completed its 2008 CIKR sector annual report in June 2008.

Within each priority, TSA listed sector-wide actions for improving CIKR protection, such as reducing the risk associated with underwater tunnels. However, it is unclear on what basis these priorities and actions were selected. For example, in the highway infrastructure and motor carrier mode, TSA and DHS leadership directed TSA's Highway Motor Carrier division to base its strategy for securing the commercial vehicle sector on the security risks posed by the shipment of hazardous materials without first conducting risk assessments to determine whether they posed the highest risk. Agency officials could not explain why TSA and DHS leadership decided to focus on hazardous materials.[33] Conducting comprehensive risk assessments would better position TSA to develop reasonable risk mitigation estimates that target the highest priority risks, inform its cost-benefit analyses, and help ensure the prioritization and selection of the most cost-effective protective programs.

Regarding the fifth step of the NIPP, TSA has implemented a number of protective programs, but without comprehensive risk assessments, the agency could not provide reasonable assurance that these programs were directed at the highest priority risks. The NIPP states that implementing protective programs based on risk assessment and prioritization enables DHS, Sector-Specific Agencies, and other security partners to enhance current CIKR protection programs and develop new programs where they will offer the greatest benefit. Without complete sector-wide risk assessments, resources may be allocated to programs designed to protect against scenarios that are of relatively lower risk. For example, TSA has not conducted an assessment of commercial aviation checkpoint screening risks to help prioritize its investments in checkpoint screening technologies. However, agency officials stated that they are currently reviewing a draft of an aviation risk assessment, known as the Air Domain Risk Assessment (ADRA), which is expected to address checkpoint security. ADRA is to provide a scenario-based risk assessment for the aviation system that may augment the information TSA uses to prioritize investments in security measures, including TSA's passenger screening program. However, TSA has not provided details on its content or its planned completion date. In the meantime, TSA has continued to invest in checkpoint screening technologies, totaling over $795 million during fiscal years 2002 through 2008. However, until ADRA or a similar risk assessment is conducted, TSA increases the possibility that such

[33] DHS determined that details on these threats are sensitive security information. Details on these threats are provided in the restricted version of this report, GAO-09-319SU.

investments will not address the highest-priority security needs in the most cost-effective manner.

In another example, although TSA had not assessed risks to the transportation sector, the agency determined that certain threats were not a high-risk focus area, that is, a high-priority threat that TSA should focus on mitigating.[34] In doing so, TSA did not follow the NIPP's approach, which calls for providing a systematic and comparable estimate of risk that can help inform sector-level risk management decisions. Instead, TSA stated that in general, intelligence, vulnerability assessments, scientific analysis, proxies for consequence, security incidents, 9/11 Commission Act requirements, and other relevant information informed TSA's determination of which threats were and were not to be high-risk focus areas. However, these activities do not meet the NIPP criteria for credible and comparable risk assessments that integrate assessments of threat, vulnerability, and consequence in a way that is documented, transparent, reproducible, and accurate. Credible risk assessments are particularly important to ensure that resources are directed to programs that address threat scenarios of relatively higher rather than relatively lower risks. Were credible and comparable risk assessments, such as those described in the NIPP, conducted for terrorism threat scenarios, the agency would be able to compare the relative risks of different types of terrorist acts.[35] The availability of such comparisons would allow TSA to prioritize its programs based on credible, systematic, and objective risk assessments. For instance, while Visible Intermodal Prevention and Response (VIPR)[36] teams and screening by Behavior Detection Officers (BDO)[37] may serve as a deterrent for improvised explosive device attacks in mass transit and aviation, they are not as likely to be as effective at providing warning for unseen biological and chemical attacks as sensors that screen air particles. Without being able to compare the relative risks of one threat scenario with another, it is unclear whether the VIPR teams and BDOs address a

[34] DHS determined that details on these threats are sensitive security information. Details on these threats are provided in the restricted version of this report, GAO-09-319SU.

[35] DHS determined that details on these threats are sensitive security information. Details on these threats are provided in the restricted version of this report, GAO-09-319SU.

[36] VIPR missions are targeted deployments of integrated TSA and other federal, state, or local assets to secure any mode of transportation. VIPR missions can occur in a variety of venues.

[37] Behavior Detection Officers are Transportation Security Officers specially trained to detect suspicious behavior in individuals in the airport environment.

threat with a relatively higher or lower risk relative to other threats, such as a chemical or biological attack. Because preventing, protecting against, responding to, or recovering from such distinct scenarios requires at times very different approaches and investments in countermeasures, without comprehensive risk assessments it is difficult for TSA to provide reasonable assurance that it is directing its programs towards the highest priority risks.

Regarding the sixth and final step of the NIPP, TSA took some steps to measure effectiveness, but without conducting comprehensive risk assessments, it could not effectively measure how its programs reduce security risks. The NIPP states that its risk management framework uses several types of performance measures to measure effectiveness, and that as the NIPP is implemented, TSA should emphasize outcome measures that track progress toward a strategic goal by documenting the beneficial results of the programs it implements. The NIPP further identifies examples of outcome measures, including (1) the reduction of risk for a specific sector measured by comparing consistent data from one year to another and (2) the overall risk mitigation achieved nationally by a particular CIKR protection initiative. Without comprehensive risk assessments, this type of analysis cannot be conducted for the transportation sector.

Despite the lack of comprehensive risk assessments, TSA made efforts to measure risk reduction for the freight rail mode. For example, TSA's freight rail mode has identified four performance metrics designed to assist the agency in gauging progress toward meeting its goals and objectives. One of these metrics specifically focused on measuring risk reduction—reducing the risk associated with the transportation of toxic inhalation hazard in major cities that have been identified as high-threat urban areas by 50 percent by the end of 2008.[38] TSA considered this metric its key overall performance indicator for the freight rail security program and reported its progress in meeting this indicator to Congress on several occasions. However, as we reported in spring 2009, TSA was unable to obtain critical data necessary to consistently measure cumulative results for this measure over the time period that it had been measuring them—

[38] The other three performance measures include (1) the number of completed rail corridor assessments in high threat urban areas; (2) the percentage of carrier adopted security action items; and (3) the percentage of employees who have received security awareness training.

2005 to 2008.[39] In particular, some baseline data needed to cumulatively calculate results for this measure are historical and could not be collected. As a result, the agency used a method for estimating risk for its baseline year that was different than what it used for calculating results for subsequent years. Thus, we recommended that TSA take steps to revise the baseline year associated with its performance measure to enable the agency to more accurately report results for this measure.

## Components of Risk Inform Resource Allocation, but without Comprehensive Risk Assessments, TSA Lacks Reasonable Assurance That Budgets Address the Highest Priority Risks

DHS policy requires TSA to use risk to inform resource allocation for the transportation sector through two avenues: the NIPP's requirement for the development of sector annual reports and DHS's budget process. The development of a sector annual report, in coordination with DHS's budget submission, is intended to inform the Office of Management and Budget (OMB), the White House, and Congress of program priorities.[40] Developing a sector annual report requires TSA to coordinate with sector partners to determine sector priorities, program requirements, and funding needs. TSA's 2008 sector annual report includes the three goals described above and associated priorities—for example, protecting the nation's transportation systems from attacks involving explosives. However, TSA had not conducted the comprehensive risk assessments necessary to inform these priorities.

Further, CIKR sector annual report guidance directs TSA to identify investments made by other federal agencies, states, or private sector security partners, where possible. TSA's 2008 annual report included information on federal spending, but did not include information on private and state investments. While TSA communicated with its partners through its government coordinating council (GCC) and modal sector coordinating councils (SCC), TSA did not use the GCC and SCCs to help identify these private and state transportation security investments.[41] TSA

[39] See GAO, *Freight Rail: Actions Have Been Taken to Enhance Freight Rail Security, but the Federal Strategy Can Be Strengthened and Security Efforts Better Monitored*, GAO-09-243SU (Washington, D.C.: spring 2009).

[40] The DHS annual budget submission is supported by the CIKR National Annual Report, which is a combination of all sector annual reports.

[41] According to the NIPP, sector-specific planning and coordination are addressed through private sector and government coordinating councils that are established for each sector. Government coordinating councils (GCC) are comprised of representatives of the sector-specific agencies, in this case, TSA; other federal departments and agencies; and state, local, and tribal governments. Sector coordinating councils (SCC) are comprised of private sector representatives.

officials acknowledged that though it is important to have reliable data on what other partners are doing to secure the transportation modes, they do not collect this type of data. Without such information, it will be difficult for TSA to avoid potentially redundant efforts in transportation security and to identify security gaps within the transportation sector that have not been addressed by federal, private sector, or state security investments.

The second avenue through which DHS policy requires TSA to use risk to inform resource allocation for the transportation sector is DHS's annual budget process—the Planning, Programming, Budgeting, and Execution (PPBE) process.[42] PPBE is a process that results in the Future Years Homeland Security Program (FYHSP), which describes DHS's resource allocation plan over 5 years as well as its annual budget request. The PPBE process recognizes that risk assessments are a key element of program plans and ultimately resource allocation, and as a component within DHS, TSA is subject to the PPBE process.[43]

To support FYHSP, DHS components play a key role in the PPBE process by providing DHS with an annual budget request and justification for funding. The funding justification, called the Resource Allocation Plan (RAP), is to provide a comprehensive expression of resources a component needs to carry out the goals, commitments, and objectives of DHS. For the components to justify their budget requests, the PPBE process requires that components review threat and vulnerability assessments; assess the status, performance, and capabilities of current programs; identify unresolved issues; and assess how they can best meet policy and planning priorities. The funding justifications must also discuss how changes in capabilities and resources affect the level of risk to the nation.[44] Components are required to articulate how risk analysis was used in these submissions to prioritize and justify activities. Components are

[42] The objective of PPBE is to articulate DHS goals, objectives, and priorities; align DHS programs to those goals; and develop and implement a program structure to accomplish those goals and objectives. FYHSP is intended to be influenced by risk assessments performed during this process.

[43] This guidance is contained in DHS Management Directive 1330.

[44] DHS has also begun to work with its components to assess risk and to evaluate the risk reduction achieved by its programs through the Office of Risk Management and Analysis' Risk Assessment Process for Informed Decision-making (RAPID). RAPID is intended to inform the program and budget phases of PPBE with strategic-level risk analysis, and is currently in the prototype phase of development.

also required to identify which DHS strategic objective and priority will be supported by any request for funding.

While this guidance instructs TSA to consider risk in the resource allocation process, TSA could not provide documentation that showed they developed budget justifications supported by risk analysis to prioritize and justify activities. TSA officials told us that, in general, program officials define vulnerabilities and advocate for resources that will allow them to mitigate those vulnerabilities through additional personnel, equipment, and operational funding. However, as previously noted in this report, while TSA's current assessment activities independently address individual components of risk, such as threat and vulnerability, they do not combine all three components of risk to create a credible risk assessment as required by the NIPP. To be considered credible, the NIPP states that risk assessments must be documented and include all three components of risk so that they can be used to support comparisons of risk, planning, and resource prioritization at the national level. To be comparable to other methodologies, the NIPP also states that risk assessments must be documented, transparent, reproducible, and accurate. Without comprehensive risk assessments, TSA lacks reasonable assurance that its long-term investments in FYHSP are allocated to the highest priority risks.

TSA officials also stated that risk is considered in the resource allocation process because TSA uses threat information to inform budget priorities. Officials said that time-critical intelligence on the imminence of a particular threat has driven budget priorities. As an example, TSA told us that in late summer of 2007, DHS and OMB submitted an amendment to the President's Budget Request for 2008 which requested funding for mitigation strategies to meet threats identified in the 2007 National Intelligence Estimate. Through this amendment, TSA received funding for additional personnel for the Aviation Direct Access Screening Program (ADASP),[45] VIPR personnel, additional K-9 teams, and additional international flight coverage by the Federal Air Marshals (FAMS). However, these budget changes were driven by assessments of threat, and the usefulness of threat information alone to inform resource allocation

[45] ADASP involves Transportation Security Officers performing security screening for explosives, incendiaries, weapons, and other prohibited items or improper airport identification media. This security screening will occur at direct access points to include secured areas, sterile areas, or aircraft operating areas outside of TSA's security screening checkpoints.

can be limited. For instance, it is impossible to know whether every threat has been identified or whether complete information about each threat has been collected. Also, a threat against a low vulnerability (hardened) facility merits a different response than the same threat made against a vulnerable facility. Thus, vulnerability and consequence assessments are essential and required to supplement threat information to better prepare for terrorist attacks.[46]

TSA officials also identified their methodology for assigning Federal Air Marshals to select flights as an example of how risk informs resource allocation at the agency. However, as we reported in January 2009,[47] the FAMS methodology is applied to one aspect of TSA's operations.[48] Further, our report noted that several improvements could be made to this methodology. Specifically, we reported that an independent review of FAMS conducted by the Homeland Security Institute recommended that FAMS refine its definition of vulnerability and increase the randomness of its flights. In response, FAMS officials stated that a new, automated, decision-support tool for selecting flights is being developed with assistance from the Homeland Security Institute and will incorporate consideration of more traditional aspects of vulnerability.[49] FAMS expects development of this tool to be completed by the end of calendar year 2009.

Without comparative risk assessments, TSA lacks reasonable assurance that risk informs the prioritization of programs within current requests across the transportation sector. Table 3 shows TSA's recent funding levels, highlighting a focus on investments in aviation security, which comprise approximately 85 percent of TSA's budget.

[46] See GAO, *Homeland Security: DHS Risk-Based Grant Methodology Is Reasonable, But Current Version's Measure of Vulnerability is Limited*, GAO-08-852 (Washington, D.C.: June 27, 2008).

[47] See GAO, *Aviation Security: Federal Air Marshal Service has Taken Actions to Fulfill its Core Mission and Address Workforce Issues, but Additional Actions are Needed to Improve Workforce Survey*, GAO-09-273 (Washington, D.C.: Jan. 14, 2009).

[48] The FAMS budget represents approximately 12 percent of TSA's total budget in fiscal year 2009.

[49] FAMS officials stated that they consulted with the aviation security community and believe that the agency's definition of vulnerability is appropriate for risk analyses relevant to the mission of FAMS.

Table 3: TSA Funding Levels for each Fiscal Year, 2007-2009

dollars in millions

| Account | FY07 | FY08 | FY09 |
|---|---:|---:|---:|
| Aviation Security | 4,732 | 4,809 | 4,755 |
| Aviation Security Capital Fund | 250 | 250 | 250 |
| Checkpoint Screening Security Fund | 0 | 250 | 0 |
| Federal Air Marshal Service | 714 | 770 | 819 |
| Threat Assessment and Credentialing | 40 | 83 | 116 |
| Surface Transportation Security | 37 | 47 | 50 |
| Transportation Security Support | 525 | 524 | 948 |
| **Total** | **6,298** | **6,733** | **6,938** |

Sources: Pub. L. No. 110-329, Div. D, 121 Stat. 3574, 3652 (2008); Pub. L. No. 110-161, Div. E, 121 Stat. 1844, 2042 (2007); Pub. L. No. 109-295, 120 Stat. 1355 (2006).

Notes: Funding levels are approximate as the amounts do not reflect rescissions, transfers, reprogrammings, carry-over balances, or supplemental appropriations. The Aviation Security Capital Fund and Checkpoint Security Screening Fund are derived from security fees collected pursuant to 49 U.S.C. § 44940 and do not constitute an actual appropriation. See 49 U.S.C. §§ 44923(h), 44940(i).

We recognize that, since the inception of TSA, other factors, such as statutory mandates, have dictated how TSA's resources have been allocated, particularly with respect to its civil aviation security responsibilities. For example, provisions of the Aviation and Transportation Security Act mandated that TSA establish a federal screening workforce within 1 year of enactment and, as amended, mandated that TSA provide for the screening of all checked baggage using explosive-detection systems by December 31, 2003.[50] More recently, the 9/11 Commission Act mandated that TSA establish a system for screening 100 percent of cargo carried on passenger aircraft.[51] Satisfying and maintaining these mandates require the continued dedication of a substantial portion of TSA's annual resources, and TSA's annual appropriation dictates many of the purposes for which its resources must be used. In addition, a wide range of decision makers influence how TSA uses its resources for transportation security, including DHS leadership, the White House, and ultimately Congress. As a result, TSA lacks the flexibility to independently allocate its resources across transportation modes solely on the basis of risk. However, through its annual budget

[50] See generally 49 U.S.C. § 44901.

[51] See 49 U.S.C. § 44901(g).

submission, TSA can propose the creation of new programs or changes to existing programs, and additional funding for any purpose authorized by law. Thus, the existence of external constraints, such as statutory mandates, does not prevent TSA from using a risk management framework to inform investment priorities and help guide future investments in security programs.

To illustrate how a risk-assessment process could help shape TSA's budget, we analyzed TSA's input to the Strategic Homeland Infrastructure Risk Assessment (SHIRA), an annual, classified DHS risk assessment, by combining TSA's vulnerability and consequence data to create a risk score for each threat scenario and then ranking each threat across all modes of transportation. We were unable to determine the reliability of TSA's data, which according to officials, were based on the judgment of subject matter experts.[52] However, TSA certifies these data to DHS as its official position and as the record of its participation in the SHIRA process. Our analysis suggests that based on TSA's data, the transportation mode that may be at highest risk is mass transit, followed by aviation, highway, freight rail, and pipeline.[53] While our analysis suggests that mass transit may be at highest risk of a terrorist attack, the highest proportion of TSA's budget is focused on aviation security.[54] It was unclear whether TSA's budget priorities were appropriately informed by risk because the agency lacks comprehensive risk assessments and information on investments in security measures by state and private sector security partners.

[52] According to TSA, these experts were informed by assessment activities (see table 2) and in lieu of risk assessments, contextual information such as passenger volume, the nature of the infrastructure (underground, underwater), time of day, and number of rail lines.

[53] The results of this analysis are dependent on the specific set of threat scenarios selected by DHS and the ratings assigned to the scenarios by TSA; the analysis does not consider the differences in the likelihood of occurrence since these data have not been provided by DHS. For example, if the set of scenarios selected by DHS were to include a more comprehensive set of likely threats, our analysis may produce different results.

[54] Our analysis suggests that TSA's budget may not reflect the risk information they are currently reporting via SHIRA to DHS, and in turn, to the White House and Congress. TSA has acknowledged the high risk to mass transit in its TS-SSP by citing a Brookings Institution study that stated "from 1991 to 2001, 42 percent of all terrorist attacks worldwide have targeted rail systems or buses."

## TSA Uses an Intelligence-Driven Approach to Risk Management Due to Concerns about the Costs of Implementing the NIPP and Reported Methodological Limitations

TSA officials told us that the agency uses an intelligence-driven approach to risk management to guide strategic investment decisions across the transportation sector because of concerns about the high cost of implementing the NIPP and the methodological limitations of this approach.[55] Although TSA committed to using the risk management framework in the NIPP with the issuance of the TS-SSP in 2007, officials reported that they encountered two main challenges that prevented them from using the NIPP framework. First, TSA officials cited that it is costly and time consuming to follow the NIPP's risk management framework—particularly in conducting comprehensive vulnerability and consequence assessments. For example, TSA's pipeline division conducts corporate security reviews that collect information on the vulnerabilities of pipelines. According to TSA officials, a pipeline corporate security review can take days to complete. TSA's pipeline division stated that they would like more staff in order to conduct its corporate security reviews more frequently. TSA officials also stated that analyzing secondary or indirect consequences of a terrorist attack and developing strategic risk objectives required much time and effort.

While TSA officials reported that it was challenging to follow the NIPP's risk management framework because it would be costly, they were not able to provide estimates of the time and resources needed to do so.  For example, TSA does not have a plan specifying the degree to which risk assessments of the sector are needed, the scope of the risks assessments, the appropriate level of resources required to complete these assessments, and time frames for completing its risk assessment efforts. However, having such a plan would help TSA identify the needed time and resources to implement the NIPP requirements. Standard practices in program management include, among other things, defining the program's scope, roles, and responsibilities, and developing a road map that establishes an order for executing projects within a specified time frame.[56] Without a plan to identify the scope, resource requirements, and timeline for risk assessments within the transportation sector, it is difficult to ensure that TSA focuses its risk assessments on the highest priorities and conducts them in a timely and cost-effective manner.

[55] TSA Risk Management Methodology, December 9, 2008.

[56] See GAO-08-492.

TSA officials cited a second challenge that prevented them from implementing the NIPP framework. TSA officials said they do not believe that a traditional risk assessment methodology—such as that provided for in the NIPP—provides a reliable method for determining the likelihood of terrorist attacks given the adaptive nature of terrorists.[57] Because terrorists adapt their tactics in response to countermeasures, TSA contends that threat assessments that quantify the likelihood of a terrorism scenario have limited value because any numerical value assigned to threats could be invalid by the end of the day.[58] Additionally, TSA contends that the traditional method of identifying terrorism scenarios is flawed because unlikely yet highly consequential threats that have never occurred cannot be anticipated and will not be included in a threat assessment.[59] For example, prior to 9/11, an attack using a plane as a weapon would have been viewed as unlikely.

Rather than using the methodology established in the NIPP for assessing risk, TSA officials stated that the agency uses an intelligence-driven approach to make strategic investment decisions across the transportation sector.[60] Within this intelligence-driven approach for the sector, TSA also developed a tactical, threat-based process known as Objectively Measured Risk Reduction (OMRR) at the program or modal level to help each of its individual modal divisions to manage their day-to-day security operations. These approaches differ from the NIPP in part because they rely primarily on intelligence information to identify threats, prioritize tactics, and guide long-term investments, rather than systematically assessing the

[57] According to this view, unlike natural disasters, when one avenue of attack is deterred by a countermeasure, terrorists will find a new mode of attack, shifting their focus to other vulnerable areas of the transportation sector.

[58] According to TSA officials, TSA's rejection of the NIPP's risk management framework in favor of an intelligence-driven approach is based in part on the assumption that risk assessment is intended to precisely predict terrorist threats. However, this assumption is inconsistent with the purpose of risk assessment, which is to provide a tool for prioritizing which assets require greater protection relative to finite resources. As we reported in December 2005, although agencies may not have enough information to identify and characterize all threats related to their assets, known or imagined adverse events should be characterized in some detail based on an understanding of an adversary's capabilities and intentions.

[59] TSA's Risk Management Methodology refers to such an event as "a low probability, high consequence event beyond the realm of normal expectations which is typically unpredicted and unpredictable. The Great Depression, the fall of the Soviet Union, and 9/11 are all examples."

[60] TSA Risk Management Methodology, December 9, 2008.

vulnerabilities and consequences of a range of threat scenarios. TSA officials stated that they will revise and reissue TS-SSP to reflect the adoption of their intelligence-driven methodology, as required by DHS,[61] but were unable to provide a date by which it will be reissued or a date by which their new methodology and risk management approach will be submitted to DHS for review and approval.[62] However, TSA officials said that they would likely not revise TS-SSP to reflect their intelligence-driven approach and submit it for review until late 2010 when the new leadership at DHS would have time to review it. Until TSA works with DHS to validate its risk management approach, TSA lacks assurance that its approach provides the agency and DHS information needed to guide investment decisions to ensure resources are allocated to the highest risks. Establishing a plan and time frame for assessing the appropriateness of TSA's intelligence-driven risk management approach could help ensure that it completes this step in a timely manner.

Although intelligence is necessary to inform threat assessments, it does not provide all of the information needed to assess risk, in particular information needed to conduct some of the vulnerability and consequence assessments that TSA lacks. In addition, the intelligence-driven approach that TSA uses may be limited because, in contrast with practices adopted by the intelligence community and the Department of Defense, TSA officials do not plan to assign uncertainty or confidence levels to the intelligence information it uses to identify threats and guide long-range planning and strategic investment. Both Congress and the administration have recognized the uncertainty inherent in intelligence analysis and have required analytic products within the intelligence community to properly

[61] DHS guidance directs sector-specific agencies like TSA to update DHS on changes to its sector specific plan, including changes in risk assessment methodologies.

[62] See GAO-09-57; see also GAO-09-243SU. TS-SSP includes annexes for each transportation mode describing how the mode would achieve the objectives and priorities established in TS-SSP. In both of these products, we reported that the annexes for the freight rail mode and the highway motor carrier mode lacked some key characteristics of successful national strategies. For example, we reported that the highway modal annex did not provide details on how sector partners will collaborate on information sharing. Similarly, we reported that the freight rail annex did not clearly identify roles and responsibilities within the freight rail mode or provide milestones for most of its programs and activities.

caveat and express uncertainties or confidence in analytic judgments.[63] TSA's intelligence products do not ascribe confidence levels to its analytic judgments. In addition, TSA officials stated that TSA does not have plans to include confidence levels in future analytic products because there do not appear to be well-established best practices within the intelligence community on how to define and use confidence levels. However, the National Intelligence Council uses a method of ascribing high, medium, or low levels of confidence to its National Intelligence Estimates, and the military intelligence community has also adopted a process for ascribing confidence levels in analytical judgments.[64] Furthermore, while intelligence can and does help the U.S. security community on an operational or tactical level to anticipate and disrupt terrorist plots, uncertainty in intelligence analysis limits its utility for long-range planning and strategic investment. Without expressing confidence levels in its analytic judgments, it will be difficult for TSA to correctly prioritize its tactics and long-term investments based on uncertain intelligence.

While TSA officials stated that they do not believe that a traditional risk assessment methodology provides a reliable method for determining the likelihood of terrorist attacks given the adaptive nature of terrorists, it is important to note that risk assessment is an accepted and required practice with a long history of use in a wide variety of public and private sector organizations. Also, the consistent assessment of risk is necessary to allow comparison of risk across and within sectors. Specifically, other agencies conduct risk assessments based on threat, vulnerability, and consequences and have overcome the challenges TSA cited. For example, within DHS, the U.S. Coast Guard and the Federal Emergency

[63] See Pub. L. No. 108-458, § 1019, 118 Stat. at 3671-72 (requiring the Director of National Intelligence to assign an individual or entity with responsibility for ensuring that finished intelligence products produced by any element or elements of the intelligence community are timely, objective, independent of political considerations, based upon all sources of available intelligence, and employ the standards of proper analytic tradecraft). See also Intelligence Community Directive 203, which establishes Intelligence Community Analytic Standards, including that analytic products: "Exhibit Proper Standards of Analytic Tradecraft, Specifically...[that each product]...properly caveats and expresses uncertainties or confidence in analytic judgments. Analytic products should indicate both the level of confidence in analytic judgments and explain the basis for ascribing it. Sources of uncertainty—including information gaps and significant contrary reporting—should be noted and linked logically and consistently to confidence levels in judgments. As appropriate, products should also identify indicators that would enhance or reduce confidence or prompt revision of existing judgments."

[64] See JP 2-0, Joint Intelligence, June 22, 2007: http://www.dtic.mil/doctrine/jel/new_pubs/jp2_0.pdf.

Management Agency (FEMA) use traditional risk assessment methodologies to inform resource allocation:[65]

- The U.S. Coast Guard, which is responsible for securing the maritime transportation mode, conducts risk assessments using its Maritime Security Risk Analysis Model (MSRAM). Used by every Coast Guard unit, MSRAM assesses the risk of terrorist attack based on scenarios—a combination of target and attack mode—in terms of threats, vulnerabilities, and consequences to more than 18,000 targets. MSRAM combines these assessments and provides analysis to identify security priorities and support risk management decisions at the strategic, operational, and tactical levels. The tool's underlying methodology is designed to capture the security risk facing different types of targets spanning every DHS CIKR industry sector, allowing comparison between different targets and geographic areas at the local, regional, and national levels. In conducting assessments, the Coast Guard Intelligence Coordination Center quantifies threat as a function of intent (the likelihood of terrorists seeking to attack), capability (the likelihood of terrorists having the resources to attack), and presence (the likelihood of terrorists having the personnel to attack).[66] Intelligence Coordination Center officials stated that the Coast Guard uses MSRAM to inform allocation decisions, such as the deployment of local resources and grants.

- We have reported that FEMA used a reasonable risk assessment methodology, based on a definition of risk as a function of threat, vulnerability, and consequence, to determine grant funding allocations under the Homeland Security Grant Program (HSGP).[67] We found that this program used a reasonable methodology to assess risk and allocate grants to states and urban areas even though its assessment of vulnerability was limited. The risk assessment methodology used by

[65] In addition to the U.S. Coast Guard and FEMA, DHS's Office of Science and Technology has conducted the following risk assessments using traditional methodologies: a Biological Threat Risk Assessment and an Integrated Chemical, Biological, Radiological, and Nuclear Terrorism Risk Assessment.

[66] According to officials from the Intelligence Coordination Center, they use intelligence to quantify each sub-element within capability, intent, and presence. For example, presence is composed of two sub-elements—the number of known or suspected extremists and the number of areas of potential support or permissive environments—which are quantified and weighted within the overall threat model. This threat assessment is combined with assessments of vulnerability and consequence to produce MSRAM's risk assessment.

[67] See GAO-08-852.

> FEMA is based on assessments of threat, vulnerability, and consequences of a terrorist attack to each state and the largest urban areas. FEMA's methodology estimates the threat to geographic areas based on terrorists' capabilities and intentions, as determined by intelligence community judgment and data on credible plots, and planning and threats from international terrorist networks. Because this threat information is recognized as uncertain, threat accounts for 20 percent of the total risk to a geographic area, while vulnerability and consequence account for 80 percent.[68]

DHS plans to enhance coordination of risk management throughout the department using an Integrated Risk Management process that accommodates the NIPP framework. In January DHS approved a new, department-wide Interim Integrated Risk Management Framework document that provides a vision, principles, overarching risk management cycle, and objectives for risk management at DHS. Implementation of the framework will include promulgation of analytical guidelines for conducting risk assessments.

## Establishing Effective Internal Controls Would Help Enforce TSA's Implementation of the NIPP's Risk Management Framework

TSA could strengthen its internal controls to help implement the NIPP's risk management framework. An organizational structure with a focal point and clearly defined roles and responsibilities would help organize TSA's efforts to implement the framework. Further, policies, procedures and guidance that require the use of the NIPP's risk management framework would aid in its implementation. Finally, a mechanism to monitor the implementation of the NIPP's risk management framework would help ensure that results are achieved and performance improved.

[68] See GAO-08-852. According to DHS officials, the agency's Office of Intelligence and Analysis (I&A) calculated the Threat Index by (1) collecting qualitative threat information with a nexus to international terrorism, (2) analyzing the threat information to create threat assessments for states and urban areas, (3) empanelling intelligence experts to review the threat assessments and reach consensus as to the number of threat tiers, and (4) assigning threat scores. This process, according to DHS officials, relied upon analytical judgment and interaction with the Intelligence Community, as opposed to the use of total counts of threats and suspicious incidents to calculate the Threat Index for the 2006 grant cycle. The final threat assessments are approved by the Intelligence Community—the Federal Bureau of Investigation, Central Intelligence Agency, National Counterterrorism Center, and the Defense Intelligence Agency—along with the DHS Under Secretary for Intelligence and Analysis and the Secretary of DHS, according to DHS officials.

## Having a Focal Point and Clearly Defined Roles and Responsibilities Would Strengthen TSA's Implementation of Risk Management Activities

While TSA acknowledged the need for a focal point to ensure implementation of risk management activities, TSA has not yet established such a focal point. *Standards for Internal Control in the Federal Government* state that an agency's organizational structure provides management's framework for planning, directing, and controlling operations to achieve agency objectives.[69] Further, internal control standards state that this structure should clearly define key areas of authority and responsibility and establish appropriate lines of reporting.

Public and private sector organizations have developed organizational structures that can contribute to effective risk management practices. In October 2007, we convened a forum of national and international experts to advance a national dialogue on applying risk management principles to homeland security.[70] Participants discussed effective risk management practices used in the public and private sectors. One practice they discussed was the concept of a chief risk officer, an executive responsible for focusing on understanding information about risks and reporting this information to senior executives. One key practice for creating an effective chief risk officer, participants said, was defining reporting relationships within the organization in a way that provides sufficient authority to hold the organization, including its highest levels, accountable to the framework and to support risk-based approaches. This practice is also consistent with internal control guidance and standards that state that organizational structure should be appropriately centralized with clearly defined key areas of authority and responsibility, and appropriate lines of reporting. A focal point—like a chief risk officer, for example—would provide an organizational structure that helps incorporate risk-informed decision making into its operations.

Although TSA officials acknowledged that a focal point would enhance TSA's risk management efforts, they stated the agency has not yet established such a focal point. TSA officials said they have taken some steps to define key areas of authority and responsibility for risk management but that more could be done. For example, in September 2008, TSA's Office of Transportation Sector Network Management (TSNM) issued a risk management directive to implement its tactical risk management methodology, OMRR. The directive establishes TSNM's

[69] See GAO/AIMD-00-21.3.1.

[70] See GAO, *Highlights of a GAO Forum: Strengthening the Use of Risk Management Principles in Homeland Security*, GAO-08-627SP (Washington, D.C.: Apr. 15, 2008).

Assistant Administrator as the official responsible for reducing the risk of terrorist attacks within the transportation sector, as well as for developing and implementing the OMRR methodology and serving as the lead official for coordinating OMRR activities among public and private sector stakeholders. However, this effort has not yet provided a focal point for TSA's risk management activities, nor does it ensure that the six steps of the NIPP's framework are implemented. For instance, the directive does not provide the Assistant Administrator with authority over staff in other offices or divisions conducting risk analysis, such as TSA's Office of Intelligence (OI), or define the relationship between OI and TSNM. In another example, TSA officials stated that they plan to establish a Risk Management Executive Steering Committee to serve as a focal point. The committee is to be charged with conducting oversight for TSA's risk management strategy, communications, and related activities, as well as with coordinating major projects and issues. However, as of December 2008, TSA had not completed a charter stating the purpose of the committee, determined its membership, established clear and appropriate lines of reporting, or held any meetings, and could not provide a date for when these actions would be completed. Further, in spring 2008, TSA disbanded its Office of Risk Management and Strategic Innovation (RMSI), which was responsible for developing risk analyses that followed the NIPP's methodology and served as a liaison between DHS's risk management offices and academic communities, among other things.[71] Since that time, TSA has not clearly defined roles and responsibilities for implementing the NIPP framework. Without a focal point for risk management that has clearly defined authority, responsibility, and appropriate lines of reporting, TSA will not have an organizational structure to direct and control activities required by the NIPP's risk management framework.

[71] RMSI developed a strategic risk management framework and the May 2007 Transportation Systems Sector-Specific Plan (TS-SSP). It also worked on the National Transportation Sector Risk Analysis (NTSRA), which was intended to be a risk assessment for the entire transportation sector. RMSI staff also worked with Boeing on the development of the Risk Management Analysis Process, a tool for evaluating the effectiveness of countermeasures in the commercial aviation sector.

## Establishing Policies, Procedures, or Guidance Would Help TSA Require the Use of the NIPP's Risk Management Framework and Specify How to Use It

TSA had not established policies, procedures, or guidance that require the use of the NIPP's risk management framework and that provide specific direction on how to use the framework. Internal control standards state that managers should take actions, such as establishing policies, procedures, and guidance, to help ensure the agency's directives are carried out, specifically, in this case, that a risk management framework is implemented and related work activities completed. Further, control activities are an integral part of an entity's planning, implementing, reviewing, and accountability for stewardship of government resources and achieving effective results. TSA lacks policies and procedures, such as a management directive, that would provide specific guidance on how to use a risk management framework, including specific guidance on how to conduct risk assessments and aggregate and analyze risk assessment results to develop a comprehensive picture of asset, system, and network risk.

In September 2008, TSNM issued a directive containing policies and procedures for implementing OMRR, TSA's threat-based and tactical approach to assessing risk at the program or modal level. However, this directive does not provide additional guidance on how to implement the six steps of the NIPP's risk management framework within TSA to inform resource allocation and long-term planning for the sector. Further, there are no mechanisms that enforce DHS's requirements, such as documenting the completion of risk assessments that meet the criteria the NIPP establishes. Without implementing such controls, TSA cannot provide reasonable assurance that it has taken the necessary steps to address risks consistently across all modes of transportation.

## Internal Monitoring Would Help TSA Implement the NIPP's Risk Management Framework

In addition, TSA has not established a mechanism to monitor how effectively the agency has implemented its risk management framework and used these results to improve its performance. According to internal control standards, monitoring should assess the quality of performance over time and ensure that the findings of audits and other reviews are promptly resolved. Managers are to promptly evaluate findings from audits and other reviews, including those showing deficiencies and recommendations, determine proper actions in response, and complete, within established time frames, all actions that correct or otherwise resolve the matters brought to management's attention. In addition, step six of the NIPP risk management framework requires agencies to measure progress and assess the effectiveness of these efforts in reducing risk.

TSA officials stated that they monitor the agency's effectiveness in implementing a risk management framework and identified their submission to the DHS Secretary's Priority Tracker, a report prepared for the Secretary on a monthly basis, as their monitoring mechanism. To prepare their monthly submission, TSA officials collect information from the modes, such as the status of strategic risk objective development and participation in the prioritized critical infrastructure list process. However, providing status updates for the Priority Tracker does not provide a mechanism to monitor how effectively the agency has implemented its risk management framework or to identify how TSA might improve its performance for several reasons. First, the scope of the information collected to update the Secretary's Priority Tracker does not include key information that would be needed to monitor TSA's progress in completing all of the steps in the NIPP's risk management framework. For example, information included in the Tracker includes participation in the prioritized critical infrastructure list process rather than information on the progress or the status of efforts to complete key risk assessment activities, including threat, vulnerability, and consequence assessments within each transportation mode. Second, these monthly submissions provide status reports but do not measure how effectively TSA has implemented a risk management framework to reduce risk. Third, these monthly status reports do not identify ways in which TSA could more effectively implement a risk management framework or better use risk management principles to guide resource allocation. Without establishing controls to monitor the effectiveness of its risk management efforts, TSA misses an opportunity to measure, evaluate, and improve its risk management activities.

## Conclusions

Using risk management principles to help set priorities and guide investments in homeland security programs can be challenging for a number of reasons, including those identified by TSA, such as the difficulty of identifying and assessing the risks posed by terrorism. However, TSA's choice to implement an intelligence-driven approach to risk management departs from GAO's and DHS's frameworks for risk management. TSA's current approach lacks assurance that it provides the agency and DHS information needed to guide investment decisions to ensure resources are allocated to the highest risks. Establishing a plan and time frame for DHS's review could help TSA ensure it obtains this important information. Further, it is important that TSA abide by the core principles of risk management to inform the annual budget process and to develop a long-term strategic investment strategy that changes over time as needed to reflect progress made in mitigating risks of terrorist attacks.

These core principles would cover, at a minimum, setting security goals and conducting comprehensive risk assessments to include threat, vulnerability, and consequence. In addition, establishing a plan and milestones for conducting risk assessments that identify the scope and resource requirements for risk assessments could help TSA ensure that it completes these key tasks. Additionally, establishing an approach to gathering data on state and private sector investments in transportation security would add to TSA's understanding of how to allocate limited resources to the highest priorities. Moreover, assigning uncertainty or confidence levels to its analytic intelligence products will permit TSA to improve the prioritization of its tactics and long-term investments. Finally, strengthening internal controls for risk management at TSA would help to ensure accountability for achieving results.

## Recommendations for Executive Action

To promote the effective use of risk management at TSA, we recommended in the restricted version of this report that the Assistant Secretary of TSA take the following six actions:

- To help provide assurances that resources are allocated to the highest priority risks across the transportation sector, better ensure that its risk management approach includes
  - adopting security goals that define specific outcomes, conditions, end points, and performance targets; and
  - conducting comprehensive risk assessments for the transportation sector that meet the NIPP criteria and combine individual assessments of threat, vulnerability, and consequence and analyzing these assessments to produce a comparative analysis of risk across the entire transportation sector to guide current and future investment decisions.
- Establish an approach for gathering data on state and private sector security partners' investments in transportation security.
- Establish a plan and milestones for conducting risk assessments for the transportation sector that identify the scope of the assessments and resource requirements for completing them.
- Work with DHS to validate its risk management approach by establishing a plan and time frame for assessing the appropriateness of TSA's intelligence-driven risk management approach for managing risk at TSA and document the results of this review once completed.
- Work with the Director of National Intelligence to determine the best approach for assigning uncertainty or confidence levels to analytic intelligence products and apply this approach to intelligence products.
- Establish internal controls, including

- a focal point and clearly defined roles and responsibilities for ensuring the risk management framework is implemented;
- policies, procedures, and guidance that require the implementation of its framework and completion of related work activities; and
- a system to monitor and improve how effectively the framework is being implemented.

## Agency Comments

We provided a draft of our restricted report to DHS and TSA for review and comment. In March 2009, DHS and TSA provided written comments, which are presented in Appendix IV. In commenting on our report, DHS and TSA stated that they agreed with our recommendations, and TSA identified actions planned or underway to implement them.

In its comments, TSA recognized the importance of resources being allocated to the highest priority risks across the transportation sector and stated that security goals will be developed and that comprehensive risk assessments will be conducted in the aviation and highway modes this calendar year. TSA also agreed to expand this approach across all modes and then integrate the results into a comparative risk analysis across the transportation sector. In addition, TSA stated that it would establish an approach for gathering data on state and private sector security partners' investments in transportation security. TSA also agreed to establish a plan and milestones for conducting risk assessments for the transportation sector that identify the scope of the assessments and resource requirements for completing them. Further, TSA agreed to work with the National Protection and Programs Directorate, Office of Risk Management and Analysis to validate TSA's current and future risk management approach and to work with the Director of National Intelligence to determine the best approach for including uncertainty or confidence levels in TSA analytic intelligence products and to apply this approach.

Finally, TSA stated that it has established an Executive Risk Management Steering Committee (ERSC) that will have overarching responsibility for managing, overseeing, and coordinating all risk analysis and risk-related management activities, including helping to frame important trade-offs for senior decision makers. However, it will be important that TSA complete a charter stating the purpose of the committee, determine its membership, establish clear and appropriate lines of reporting, and begin to hold ERSC meetings in the near future. It will also be important that the ERSC establish policies, procedures, and guidance that require the implementation of TSA's risk management framework and completion of related work activities and that it establish a system to monitor and improve how effectively the framework is being implemented.

DHS and TSA also provided us with technical comments, which we considered and incorporated in the report where appropriate.

As agreed with your office, unless you publicly announce the contents of this report, we plan no further distribution for 30 days from the report date. At that time, we will send copies of this report to the Secretary of Homeland Security, the Assistant Secretary of the Transportation Security Administration, and appropriate congressional committees. In addition, this report will be available at no charge on the GAO Web site at http://www.gao.gov/.

If you or your staff have any questions about this report or wish to discuss these matters further, please contact me at (202) 512-4379 or lords@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix V.

Sincerely yours,

Stephen Lord

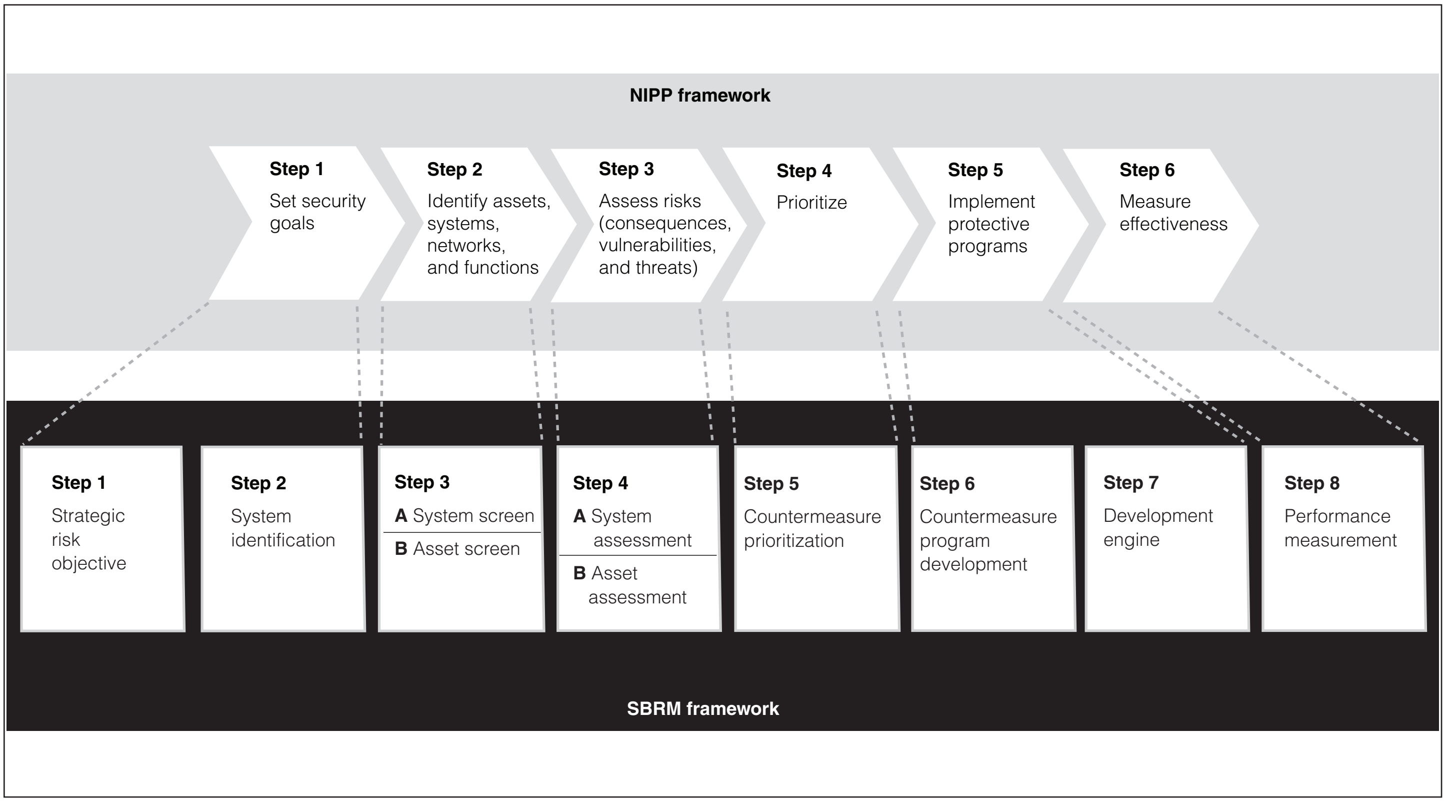
Stephen M. Lord
Director, Homeland Security and Justice Issues

# Appendix I: Transportation Security Administration (TSA) Risk Management Frameworks

TSA developed a strategic risk management framework that aligns with the National Infrastructure Protection Plan's (NIPP) risk management framework but decided not to implement it to guide resource allocation. While the NIPP does not require that TSA develop an additional framework, TSA developed its own strategic risk management framework to tailor the NIPP framework to the transportation system. In May 2007, TSA issued the Transportation Systems Sector-Specific Plan (TS-SSP), as well as supporting annexes for the aviation, freight rail, highway, maritime, mass transit, and pipeline modes. This plan and its supporting modal annexes and appendices describe the security framework that is to enable sector stakeholders to make effective, risk-informed security and resource allocation decisions.

A key component of TS-SSP is TSA's Systems-Based Risk Management (SBRM) framework, which is a structured, eight-step approach for implementing the plan. According to TS-SSP, this framework was not designed for operational or tactical planning.  Instead, SBRM was developed to augment the NIPP and looks beyond protecting a single asset or set of assets by taking a systems view of risk to address the complex and interconnected nature of the systems that comprise the transportation network. According to TSA, this strategic, systems-level approach is vital to providing security to the transportation sector because consequences of system-level failure can far exceed consequences associated with single assets. Figure 3 describes how the eight steps of SBRM align with the six steps of the NIPP.

Figure 3: Alignment between the NIPP and TSA's Systems-Based Risk Management Framework (SBRM)


NIPP framework
Step 1 Set security goals
Step 2 Identify assets, systems, networks, and functions
Step 3 Assess risks (consequences, vulnerabilities, and threats)
Step 4 Prioritize
Step 5 Implement protective programs
Step 6 Measure effectiveness
Step 1 Strategic risk objective
Step 2 System identification
Step 3 A System screen B Asset screen
Step 4 A System assessment B Asset assessment
Step 5 Countermeasure prioritization
Step 6 Countermeasure program development
Step 7 Development engine
Step 8 Performance measurement
SBRM framework

Sources: GAO presentation of DHS and TSA information.

According to TSA officials, the NIPP's risk management framework does not produce actionable information for their day-to-day operations, and they instead have developed what they refer to as an "intelligence-driven" approach to risk management. Although with the issuance of TS-SSP in 2007 TSA committed to use the risk management framework in the NIPP, its experience trying to implement the risk management framework to guide selection of programs and investments since then has led TSA to conclude the agency should follow an intelligence-driven approach to risk management. TSA officials also stated that they plan to replace SBRM with the intelligence-driven methodology as part of its reissuance of TS-SSP, but they did not provide specific details on when they will reissue TS-SSP or whether the new methodology will be first approved by DHS.

Within this intelligence-driven approach, TSA has developed a process for assessing risk known as Objectively Measured Risk Reduction (OMRR). TSA officials explained that OMRR is meant to assist in their day-to-day efforts addressing immediate risks rather than serving as a strategic framework for the overall transportation sector. TSA officials emphasized the value and relative ease of using OMRR rather than the agency's strategic risk management framework. TSA officials stated that all of the modal divisions within TSA's office of Transportation Security Network Management are expected to use OMRR, although it does not align with the steps of the risk management framework in the NIPP.

# Appendix II: Detailed Summary of TSA's Current Assessment Activities

| | Program activity | | Risk information provided | | | Risk assessment conducted (including threat, vulnerability, and consequence)[a] |
|---|---|---|---|---|---|---|
| Mode | Title | Description | Threat | Vulnerability | Consequence | |
| Multiple modes | Administrators Daily Intelligence Briefing | Provides a 24-hour snapshot of transportation-related intelligence. | Yes | No | No | No |
| | Homeland Information Report | Provides intelligence information to the intelligence and law enforcement communities. | Yes | No | No | |
| | Note to Administrator | Provides information on a specific request from the Administrator on a topic of interest. | Yes | No | No | |
| | Strategic Homeland Infrastructure Risk Assessment | Classified report developed by DHS's Homeland Infrastructure Threat Assessment Center that provides an overview of current high-risk scenarios across all critical infrastructure and key resources sectors. Transportation Sector Network Management's (TSNM) modal divisions contribute vulnerability and consequence analysis. | No | Yes | Yes | |
| | Spot Reports | Share time-sensitive information and provide situational awareness on individuals denied boarding or in flight, people of interest to the law enforcement or intelligence community, or an event important to TSA's mission. | Yes | No | No | |
| | Special Event Threat Assessments | Provide in-depth analysis of potential threats with a transportation focus. | Yes | No | No | |
| | Transportation Intelligence Gazettes | Provide in-depth analysis focused on a specific topic within a transportation mode. | Yes | No | No | |
| | Transportation Suspicious Incidents Report | Provides analysis of suspicious activities and surveillance directed against all transportation modes. | Yes | No | No | |

| | Program activity | | Risk information provided | | | Risk assessment conducted (including threat, vulnerability, and consequence)[a] |
|---|---|---|---|---|---|---|
| Mode | Title | Description | Threat | Vulnerability | Consequence | |
| Aviation | Air Cargo Vulnerability Assessments | Collect information on how air carriers, freight forwarders, and agents operate their businesses and on physical surroundings, such as the quality of door locks and alarms. | No | Yes | No | No |
| | Aviation Mode Annual Threat Assessment | Provides in-depth analysis of potential threats. | Yes | No | No | |
| | Current Airport Threat Assessment | Provides threat information on various classes of airports across the United States. | Yes | No | No | |
| | Joint Vulnerability Assessments | Investigate physical security elements of airports, such as fences and access controls. Conducted with cooperation from the FBI, Federal Security Directors, cargo inspectors, airport management, and other entities. The FBI independently conducts a threat assessment, and TSA independently conducts a vulnerability assessment. | No | Yes | No | |
| | Man-Portable Air Defense Systems (MANPADS) Vulnerability Assessments | Evaluate the locations from which attackers can deploy MANPADS. Conducted in cooperation with the FBI, Federal Aviation Administration, airport operators, local law enforcement, and other key stakeholders. | No | Yes | No | |
| | No-Fly/Selectee Lists | The No Fly List identifies individuals who should be prevented from boarding an aircraft. The Selectee List identifies individuals who must undergo enhanced screening at the checkpoint prior to boarding.[b] | Yes | No | No | |

| | Program activity | | Risk information provided | | | Risk assessment conducted (including threat, vulnerability, and consequence)[a] |
|---|---|---|---|---|---|---|
| Mode | Title | Description | Threat | Vulnerability | Consequence | |
| Freight rail | Corporate Security Reviews | Evaluate freight rail companies' security plans and procedures and may include site visits. | No | Yes | No | No |
| | Freight Rail Mode Annual Threat Assessment | Provides in-depth analysis of potential threats. | Yes | No | No | |
| | Rail Corridor Reviews | Determine the vulnerabilities and potential consequences toxic inhalation hazard (TIH) cars pose in major areas by identifying locations within a city's rail network where TIH cars are vulnerable to attack. | No | Yes | Yes | |
| | TIH Rail Risk Monitoring Program | Assesses the security of rail TIH transportation in 46 major urban areas using industry data about TIH car movements inside the urban area. Also audits the security status of cars while at rail yards using TSA inspectors and assess potential consequences associated with the surrounding population. | No | Yes | Yes | |
| Highway infrastructure and motor carrier | Corporate Security Reviews | Conducted with organizations engaged in transportation by motor vehicle and those that maintain or operate key physical assets within the highway transportation community. Serve to evaluate and collect physical and operational preparedness information, evaluate critical assets and key point-of-contact lists, review emergency procedures and domain awareness training, and provide an opportunity to share industry best practices. | No | Yes | No | No |
| | Highway Infrastructure and Motor Carrier Mode Annual Threat Assessment | Provide in-depth analysis of potential threats. | Yes | No | No | |

| | Program activity | | Risk information provided | | | Risk assessment conducted (including threat, vulnerability, and consequence)[a] |
|---|---|---|---|---|---|---|
| **Mode** | **Title** | **Description** | **Threat** | **Vulnerability** | **Consequence** | |
| **Mass transit** | Baseline Assessment and Security Enhancement review (BASE) | Reviews transit systems implementation of 17 security action items jointly developed by TSA and FTA in coordination with the Mass Transit Sector Coordinating Council. | No | Yes | No | No |
| | Mass Transit Mode Annual Threat Assessment | Provides in-depth analysis of potential threats. | Yes | No | No | |
| | Security Analysis and Action Program (SAAP) | Provides a systematic vulnerability assessment of mass transit or passenger rail systems. SAAPs can be conducted on individual critical infrastructure facilities or entire rail systems, with particular emphasis on critical control points. | No | Yes | No | |
| **Pipeline** | Acute Assessment | Evaluates threats to the security of selected sites. | Yes | No | No | No |
| | Corporate Security Reviews | Provide on-site reviews of pipeline security companies. | No | Yes | No | |
| | Pipeline Cross-Border Vulnerability Assessments Program | U.S. and Canadian teams assess pipeline operations, control systems, interdependencies, and assault planning in critical cross-border infrastructure. | No | Yes | No | |
| | Pipeline Mode Annual Threat Assessment | Provides in-depth analysis of potential threats. | Yes | No | No | |

Sources: TSA and GAO analysis.

[a] A risk assessment requires a combination of all three components of risk, and in these cases no efforts were made to combine the components into a comprehensive assessment.

[b] DHS determined that details on the No-Fly and Selectee Lists are sensitive security information. Details on the lists are provided in the restricted version of this report, GAO-09-319SU.

# Appendix III: GAO Analysis of TSA's SHIRA Input

The Strategic Homeland Infrastructure Risk Assessment (SHIRA) is an annual, classified product that assesses risk across and within each of the nation's 18 Critical Infrastructure and Key Resources (CIKR) sectors. To develop SHIRA, the Department of Homeland Security (DHS) works with members of the Intelligence Community to determine applicable threats against various systems and assets. TSA then assesses vulnerabilities and consequences resulting from scenarios involving these threats by providing scores and enters these data into a worksheet which TSA certifies as the official record of its position and participation in SHIRA.

The vulnerability and consequence ranking data in table 4 is derived from TSA's worksheets. We were unable to determine the reliability of this data, which according to TSA officials was based on the judgment of subject matter experts, who were informed by assessment activities (see table 2) and in lieu of risk assessments, contextual information such as passenger volume, the nature of the infrastructure (underground, underwater), time of day, and number of rail lines. However, TSA certifies these data to DHS as its official position and as the record of its participation in the SHIRA process.

Vulnerability rankings are based on countermeasure effectiveness, which are ranked on a scale of 0 to 4 as shown in table 4.

**Table 4: Ranking Scale for Countermeasure Effectiveness**

| 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| The existing countermeasures are very likely to defeat the attack (80 to 100 percent chance). | The existing countermeasures are likely to defeat the attack (60 to 80 percent chance). | The existing countermeasures are somewhat likely to defeat the attack (40 to 60 percent chance). | The existing countermeasures are unlikely to defeat the attack (20 to 40 percent chance). | The existing countermeasures are very unlikely to defeat the attack (0 to 20 percent chance). |

Source: DHS.

We used the midpoint of each of these rankings as the probability that the existing countermeasures will defeat the attack, and then subtracted this probability from 1 to determine the probability that the existing countermeasures will not defeat the attack.

Consequence rankings are also based on a scale of 0 to 4, as shown in table 5 below.

Table 5: Consequences Ranking Scales

| Ranking scale | Loss of life | Economic consequences | Psychological consequences |
|---|---|---|---|
| 0: Negligible | No fatalities | Less than $100 million | No major change in population behavior, or effects on social functioning locally or nationally. |
| 1: Minor | Less than 100 | Greater than $100 million | Occasional or minor loss of nonessential social functions in a circumscribed geographical area. |
| 2: Moderate | Greater than 100 | Greater than $1 billion | Loss of many nonessential social functions in a circumscribed geographical area. |
| 3: Significant | Greater than 1,000 | Greater than $10 billion | Dysfunctional behavior and disruption of important social functions for a sustained period. |
| 4: Severe | Greater than 10,000 | Greater than $100 billion | Loss of belief in government and institutions, widespread disregard for official instructions, widespread looting and civil unrest. |

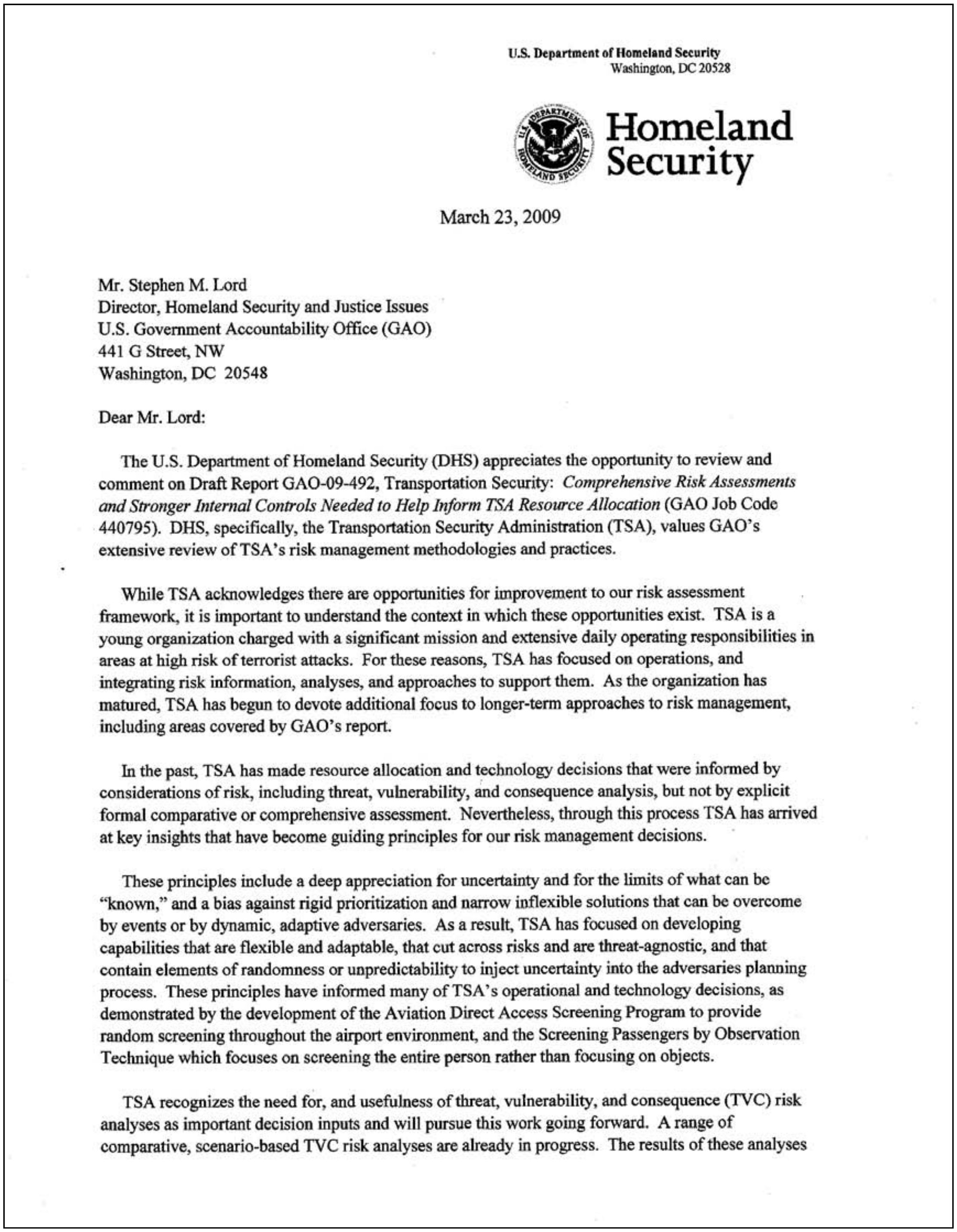
Source: DHS.

Our analysis of TSA's input to SHIRA suggests that mass transit may be at the greatest risk of a terrorist attack, followed by aviation, highway, freight rail, and pipeline.[1] The results of this analysis are dependent on the specific set of threat scenarios selected by DHS and the ratings assigned to the scenarios by TSA; the analysis does not consider the differences in the likelihood of occurrence since TSA did not assign likelihood estimates to the threat scenarios.[2] As a result, our analysis uses conditional risk values, consequence multiplied by vulnerability, as called for by the NIPP. We used similar weightings to those applied in other DHS models to weight consequence values: 60 percent for loss of life, 35 percent for economic consequences, and 5 percent for psychological consequences. We applied these weightings to the consequence values and summed them to determine the weighted consequence value for each scenario. We then calculated the risk scores for each scenario by multiplying the weighted consequences by the likelihood that existing countermeasures will defeat the scenario. Risk scores were then aggregated for each mode to determine the relative risk to each mode.

[1] DHS determined that details of our analysis of TSA's input to SHIRA are sensitive security information. Details of this analysis are provided in the restricted version of this report, GAO-09-319SU.

[2] For example, if the set of scenarios selected by DHS were to include a more comprehensive set of likely threats, our analysis may produce different results Given the lack of likelihood estimates for the threat scenarios, a test of the sensitivity of our analysis with respect to key sources of uncertainty would test the robustness of these results.

# Appendix IV: Comments from the Department of Homeland Security



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

Homeland
Security

March 23, 2009

Mr. Stephen M. Lord
Director, Homeland Security and Justice Issues
U.S. Government Accountability Office (GAO)
441 G Street, NW
Washington, DC 20548

Dear Mr. Lord:

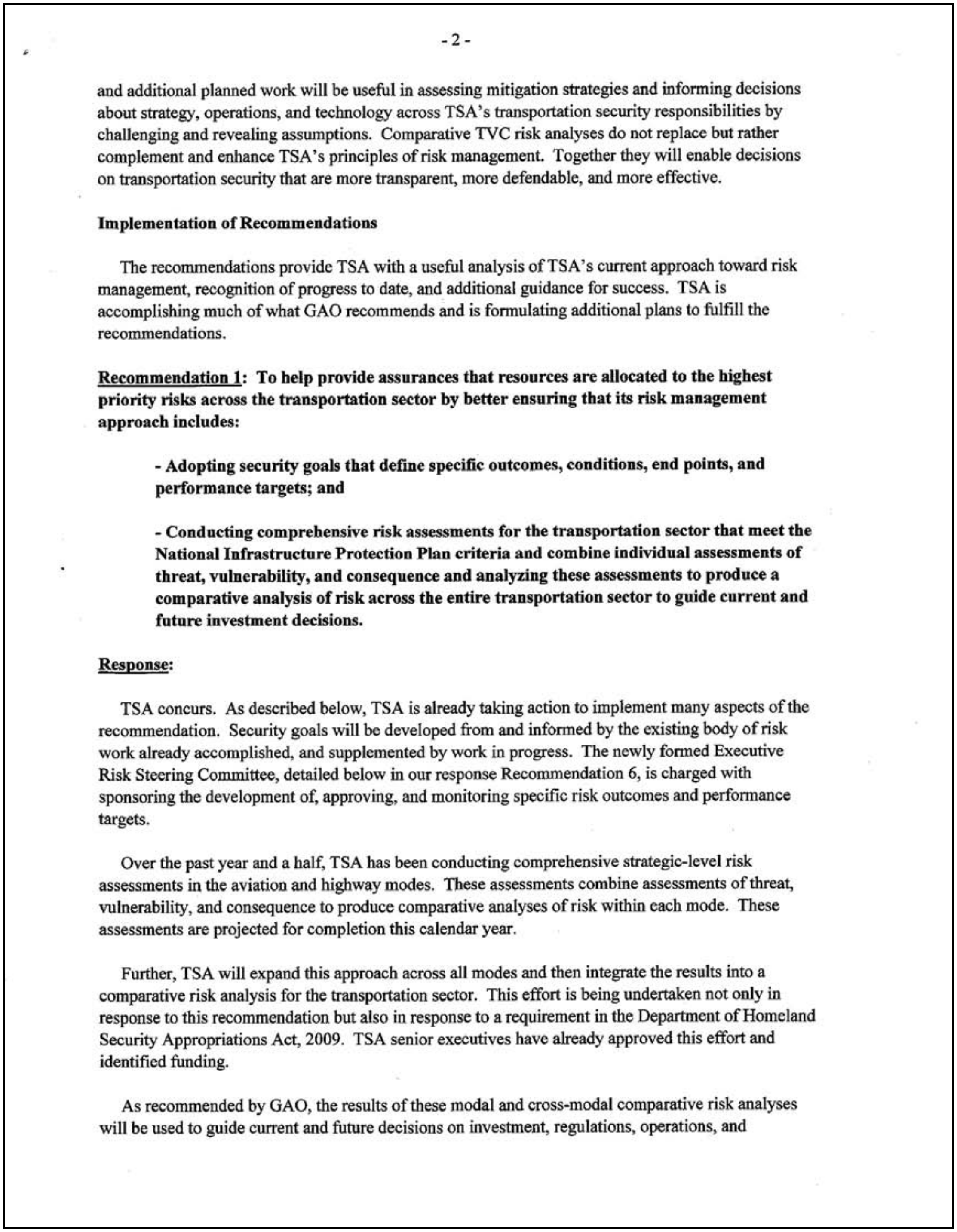
The U.S. Department of Homeland Security (DHS) appreciates the opportunity to review and comment on Draft Report GAO-09-492, Transportation Security: *Comprehensive Risk Assessments and Stronger Internal Controls Needed to Help Inform TSA Resource Allocation* (GAO Job Code 440795). DHS, specifically, the Transportation Security Administration (TSA), values GAO's extensive review of TSA's risk management methodologies and practices.

While TSA acknowledges there are opportunities for improvement to our risk assessment framework, it is important to understand the context in which these opportunities exist. TSA is a young organization charged with a significant mission and extensive daily operating responsibilities in areas at high risk of terrorist attacks. For these reasons, TSA has focused on operations, and integrating risk information, analyses, and approaches to support them. As the organization has matured, TSA has begun to devote additional focus to longer-term approaches to risk management, including areas covered by GAO's report.

In the past, TSA has made resource allocation and technology decisions that were informed by considerations of risk, including threat, vulnerability, and consequence analysis, but not by explicit formal comparative or comprehensive assessment. Nevertheless, through this process TSA has arrived at key insights that have become guiding principles for our risk management decisions.

These principles include a deep appreciation for uncertainty and for the limits of what can be "known," and a bias against rigid prioritization and narrow inflexible solutions that can be overcome by events or by dynamic, adaptive adversaries. As a result, TSA has focused on developing capabilities that are flexible and adaptable, that cut across risks and are threat-agnostic, and that contain elements of randomness or unpredictability to inject uncertainty into the adversaries planning process. These principles have informed many of TSA's operational and technology decisions, as demonstrated by the development of the Aviation Direct Access Screening Program to provide random screening throughout the airport environment, and the Screening Passengers by Observation Technique which focuses on screening the entire person rather than focusing on objects.

TSA recognizes the need for, and usefulness of threat, vulnerability, and consequence (TVC) risk analyses as important decision inputs and will pursue this work going forward. A range of comparative, scenario-based TVC risk analyses are already in progress. The results of these analyses



and additional planned work will be useful in assessing mitigation strategies and informing decisions about strategy, operations, and technology across TSA's transportation security responsibilities by challenging and revealing assumptions. Comparative TVC risk analyses do not replace but rather complement and enhance TSA's principles of risk management. Together they will enable decisions on transportation security that are more transparent, more defendable, and more effective.

**Implementation of Recommendations**

The recommendations provide TSA with a useful analysis of TSA's current approach toward risk management, recognition of progress to date, and additional guidance for success. TSA is accomplishing much of what GAO recommends and is formulating additional plans to fulfill the recommendations.

**Recommendation 1: To help provide assurances that resources are allocated to the highest priority risks across the transportation sector by better ensuring that its risk management approach includes:**

> **- Adopting security goals that define specific outcomes, conditions, end points, and performance targets; and**
>
> **- Conducting comprehensive risk assessments for the transportation sector that meet the National Infrastructure Protection Plan criteria and combine individual assessments of threat, vulnerability, and consequence and analyzing these assessments to produce a comparative analysis of risk across the entire transportation sector to guide current and future investment decisions.**

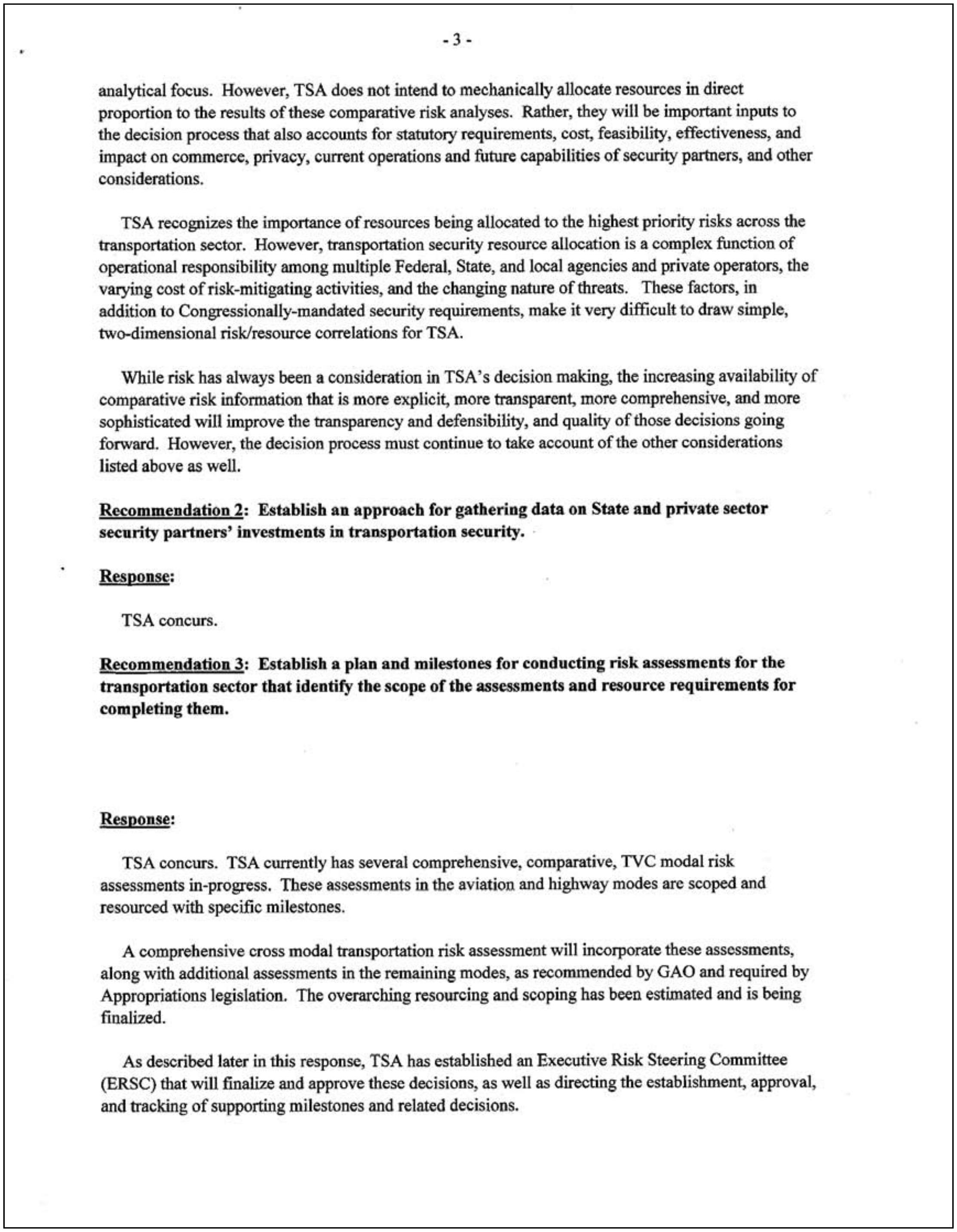
**Response:**

TSA concurs. As described below, TSA is already taking action to implement many aspects of the recommendation. Security goals will be developed from and informed by the existing body of risk work already accomplished, and supplemented by work in progress. The newly formed Executive Risk Steering Committee, detailed below in our response Recommendation 6, is charged with sponsoring the development of, approving, and monitoring specific risk outcomes and performance targets.

Over the past year and a half, TSA has been conducting comprehensive strategic-level risk assessments in the aviation and highway modes. These assessments combine assessments of threat, vulnerability, and consequence to produce comparative analyses of risk within each mode. These assessments are projected for completion this calendar year.

Further, TSA will expand this approach across all modes and then integrate the results into a comparative risk analysis for the transportation sector. This effort is being undertaken not only in response to this recommendation but also in response to a requirement in the Department of Homeland Security Appropriations Act, 2009. TSA senior executives have already approved this effort and identified funding.

As recommended by GAO, the results of these modal and cross-modal comparative risk analyses will be used to guide current and future decisions on investment, regulations, operations, and



analytical focus. However, TSA does not intend to mechanically allocate resources in direct proportion to the results of these comparative risk analyses. Rather, they will be important inputs to the decision process that also accounts for statutory requirements, cost, feasibility, effectiveness, and impact on commerce, privacy, current operations and future capabilities of security partners, and other considerations.

TSA recognizes the importance of resources being allocated to the highest priority risks across the transportation sector. However, transportation security resource allocation is a complex function of operational responsibility among multiple Federal, State, and local agencies and private operators, the varying cost of risk-mitigating activities, and the changing nature of threats. These factors, in addition to Congressionally-mandated security requirements, make it very difficult to draw simple, two-dimensional risk/resource correlations for TSA.

While risk has always been a consideration in TSA's decision making, the increasing availability of comparative risk information that is more explicit, more transparent, more comprehensive, and more sophisticated will improve the transparency and defensibility, and quality of those decisions going forward. However, the decision process must continue to take account of the other considerations listed above as well.

**Recommendation 2: Establish an approach for gathering data on State and private sector security partners' investments in transportation security.**

**Response:**

TSA concurs.

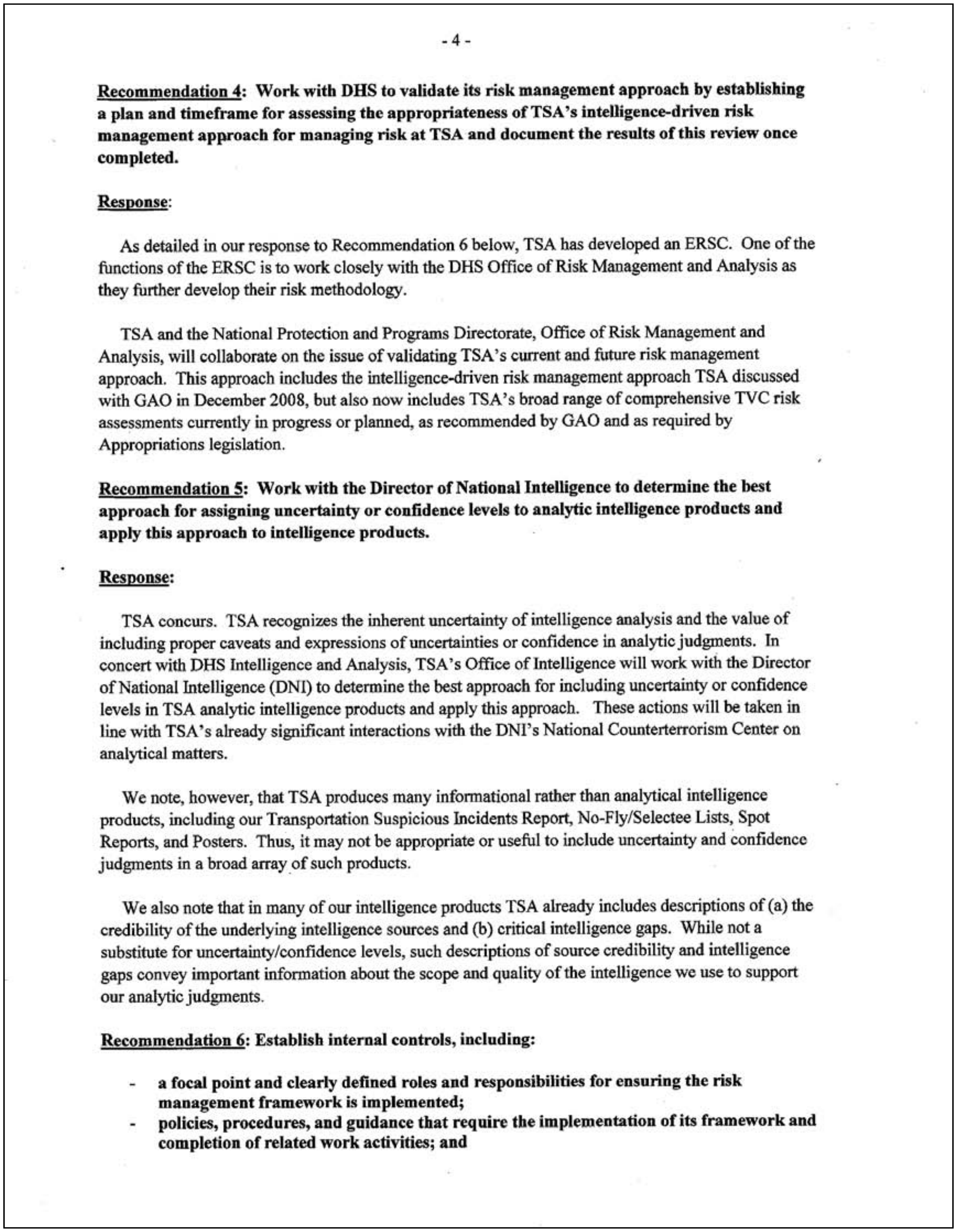
**Recommendation 3: Establish a plan and milestones for conducting risk assessments for the transportation sector that identify the scope of the assessments and resource requirements for completing them.**

**Response:**

TSA concurs. TSA currently has several comprehensive, comparative, TVC modal risk assessments in-progress. These assessments in the aviation and highway modes are scoped and resourced with specific milestones.

A comprehensive cross modal transportation risk assessment will incorporate these assessments, along with additional assessments in the remaining modes, as recommended by GAO and required by Appropriations legislation. The overarching resourcing and scoping has been estimated and is being finalized.

As described later in this response, TSA has established an Executive Risk Steering Committee (ERSC) that will finalize and approve these decisions, as well as directing the establishment, approval, and tracking of supporting milestones and related decisions.



**<u>Recommendation 4</u>: Work with DHS to validate its risk management approach by establishing a plan and timeframe for assessing the appropriateness of TSA's intelligence-driven risk management approach for managing risk at TSA and document the results of this review once completed.**

<u>Response</u>:

As detailed in our response to Recommendation 6 below, TSA has developed an ERSC. One of the functions of the ERSC is to work closely with the DHS Office of Risk Management and Analysis as they further develop their risk methodology.

TSA and the National Protection and Programs Directorate, Office of Risk Management and Analysis, will collaborate on the issue of validating TSA's current and future risk management approach. This approach includes the intelligence-driven risk management approach TSA discussed with GAO in December 2008, but also now includes TSA's broad range of comprehensive TVC risk assessments currently in progress or planned, as recommended by GAO and as required by Appropriations legislation.

**<u>Recommendation 5</u>: Work with the Director of National Intelligence to determine the best approach for assigning uncertainty or confidence levels to analytic intelligence products and apply this approach to intelligence products.**

**<u>Response</u>:**

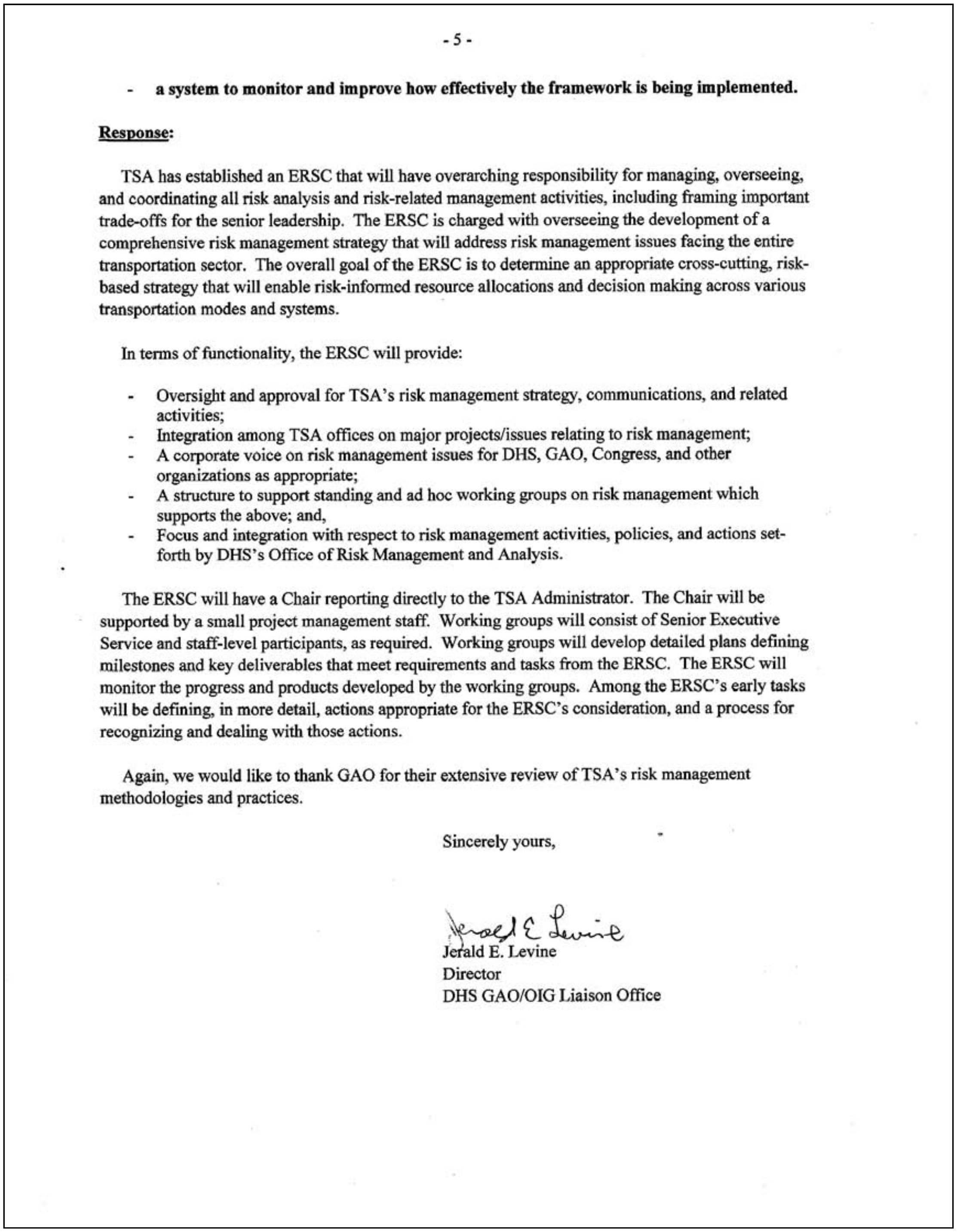
TSA concurs. TSA recognizes the inherent uncertainty of intelligence analysis and the value of including proper caveats and expressions of uncertainties or confidence in analytic judgments. In concert with DHS Intelligence and Analysis, TSA's Office of Intelligence will work with the Director of National Intelligence (DNI) to determine the best approach for including uncertainty or confidence levels in TSA analytic intelligence products and apply this approach. These actions will be taken in line with TSA's already significant interactions with the DNI's National Counterterrorism Center on analytical matters.

We note, however, that TSA produces many informational rather than analytical intelligence products, including our Transportation Suspicious Incidents Report, No-Fly/Selectee Lists, Spot Reports, and Posters. Thus, it may not be appropriate or useful to include uncertainty and confidence judgments in a broad array of such products.

We also note that in many of our intelligence products TSA already includes descriptions of (a) the credibility of the underlying intelligence sources and (b) critical intelligence gaps. While not a substitute for uncertainty/confidence levels, such descriptions of source credibility and intelligence gaps convey important information about the scope and quality of the intelligence we use to support our analytic judgments.

**<u>Recommendation 6</u>: Establish internal controls, including:**

- **a focal point and clearly defined roles and responsibilities for ensuring the risk management framework is implemented;**
- **policies, procedures, and guidance that require the implementation of its framework and completion of related work activities; and**



- **a system to monitor and improve how effectively the framework is being implemented.**

**Response:**

TSA has established an ERSC that will have overarching responsibility for managing, overseeing, and coordinating all risk analysis and risk-related management activities, including framing important trade-offs for the senior leadership. The ERSC is charged with overseeing the development of a comprehensive risk management strategy that will address risk management issues facing the entire transportation sector. The overall goal of the ERSC is to determine an appropriate cross-cutting, risk-based strategy that will enable risk-informed resource allocations and decision making across various transportation modes and systems.

In terms of functionality, the ERSC will provide:

- Oversight and approval for TSA's risk management strategy, communications, and related activities;
- Integration among TSA offices on major projects/issues relating to risk management;
- A corporate voice on risk management issues for DHS, GAO, Congress, and other organizations as appropriate;
- A structure to support standing and ad hoc working groups on risk management which supports the above; and,
- Focus and integration with respect to risk management activities, policies, and actions set-forth by DHS's Office of Risk Management and Analysis.

The ERSC will have a Chair reporting directly to the TSA Administrator. The Chair will be supported by a small project management staff. Working groups will consist of Senior Executive Service and staff-level participants, as required. Working groups will develop detailed plans defining milestones and key deliverables that meet requirements and tasks from the ERSC. The ERSC will monitor the progress and products developed by the working groups. Among the ERSC's early tasks will be defining, in more detail, actions appropriate for the ERSC's consideration, and a process for recognizing and dealing with those actions.

Again, we would like to thank GAO for their extensive review of TSA's risk management methodologies and practices.

Sincerely yours,

Jerald E Levine

Jerald E. Levine
Director
DHS GAO/OIG Liaison Office

# Appendix V: GAO Contact and Staff Acknowledgments

## GAO Contact

Stephen M. Lord, (202) 512-4379, lords@gao.gov

## Staff Acknowledgments

In addition to the contact named above, Anne Laffoon, Assistant Director, and Tony Cheesebrough, Analyst-in-Charge, managed this assignment. Jason Barnosky, Kathryn Bolduc, Maylin Jue, and David Messman made significant contributions to this work. Chuck Bausell and Stan Kostyla assisted with design, methodology, and data analysis. Katherine Davis provided assistance in report preparation; Tom Lombardi provided legal support; and Pille Anvelt and Barbara Hills developed the report's graphics.

(440795)

## GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

## Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

### Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

## Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

## Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548