

GAO

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

January 2009

HIGHWAY INFRASTRUCTURE

Federal Efforts to
Strengthen Security
Should Be Better
Coordinated and
Targeted on the
Nation's Most Critical
Highway
Infrastructure



GAO

Accountability * Integrity * Reliability



Highlights of [GAO-09-57](#), a report to the Chairman, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

The nation's highway transportation system is vast and open—vehicles and their operators can move freely and with almost no restrictions. Securing the U.S. highway infrastructure system is a responsibility shared by federal, state and local government, and the private sector. Within the Department of Homeland Security (DHS), the Transportation Security Administration (TSA) has primary responsibility for ensuring the security of the sector. GAO was asked to assess the progress DHS has made in securing the nation's highway infrastructure. This report addresses the extent to which federal entities have conducted and coordinated risk assessments; DHS has developed a risk-based strategy; and stakeholders, such as state and local transportation entities, have taken voluntary actions to secure highway infrastructure — and the degree to which DHS has monitored such actions. To conduct this work, GAO reviewed risk assessment results and TSA's documented security strategy, and conducted interviews with highway stakeholders.

What GAO Recommends

GAO recommends that DHS establish a mechanism to enhance coordination of risk assessments; TSA address limitations in its documented security strategy for highway infrastructure; and that TSA develop a mechanism to monitor security measures for critical highway infrastructure. DHS and TSA concurred with these recommendations.

To view the full product, including the scope and methodology, click on [GAO-09-57](#). For more information, contact Cathleen Berrick at (202) 512-3404 or berrickc@gao.gov.

HIGHWAY INFRASTRUCTURE

Federal Efforts to Strengthen Security Should Be Better Coordinated and Targeted on the Nation's Most Critical Highway Infrastructure

What GAO Found

Federal entities have several efforts underway to assess threat, vulnerability, and consequence—the three elements of risk—for highway infrastructure; however, these efforts have not been systematically coordinated among key federal partners and the results are not routinely shared. Several component agencies and offices within DHS and the Department of Transportation (DOT) are conducting individual risk assessment efforts of highway infrastructure vulnerabilities, and collectively have completed assessments of most of the critical highway assets identified in 2007. However, key DHS entities reported that they were not coordinating these activities or sharing the results. According to the National Infrastructure Protection Plan, TSA is responsible for coordinating risk assessment programs. Establishing mechanisms to enhance coordination of risk assessments among key federal partners could strengthen and validate assessments and leverage limited federal resources.

DHS, through TSA, has developed and implemented a strategy to guide highway infrastructure security efforts, but the strategy is not informed by available risk assessments and lacks some key characteristics GAO has identified for effective national strategies. In May 2007, TSA issued the Highway Modal Annex, which is intended to serve as the principal strategy for implementing key programs for securing highway infrastructure. While its completion was an important first step to guide protection efforts, GAO identified a number of limitations that may influence its effectiveness. For example, the Annex is not fully based on available risk information, although DHS's Transportation Systems -Sector Plan and the National Infrastructure Protection Plan call for risk information to be used to guide all protection efforts. Lacking such information, DHS cannot provide reasonable assurance that its current strategy is effectively addressing security gaps, prioritizing investments based on risk, and targeting resources toward security measures that will have the greatest impact. GAO also identified a number of additional characteristics of effective national strategies that were missing or incomplete in the current Highway Modal Annex.

Federal entities, along with other highway sector stakeholders, have taken a variety of actions to mitigate risks to highway infrastructure; however, DHS, through TSA, lacks a mechanism to determine the extent to which voluntary security measures have been employed to protect critical assets. Specifically, highway stakeholders have developed publications and training, conducted research and development activities, and implemented specific voluntary protective measures for infrastructure assets, such as fencing and cameras. However, TSA does not have a mechanism to monitor protective measures implemented for critical highway infrastructure assets, although TSA is tasked with evaluating the effectiveness and efficiency of federal initiatives to secure surface transportation modes. Without such a monitoring mechanism, TSA cannot determine the level of security preparedness of the nation's critical highway infrastructure.

Contents

Letter		1
	Results in Brief	5
	Background	9
	Federal Entities Have Initiated Efforts to Assess Risks to Highway Infrastructure, But Coordination of These Efforts is Limited	17
	DHS's Strategy to Secure Highway Infrastructure Was Not Fully Informed by Available Risk Information, and Should be Strengthened	33
	Government and Industry Stakeholders Have Efforts Underway to Enhance the Security of Highway Infrastructure, but TSA Lacks a Mechanism to Monitor Implementation of Voluntary Security Measures	44
	Conclusions	55
	Recommendations for Executive Action	57
	Agency Comments and Our Evaluation	57
Appendix I	Objectives, Scope and Methodology	62
Appendix II	Selected Laws and Federal Guidance Concerning the Security of Highway Infrastructure, 1996 to Present	66
Appendix III	Examples of Selected Protective Security Measures that Could be Implemented by Asset Owners and Operators	71
Appendix IV	Summary of Selected Federal and Non-Federal Research and Development Programs to Enhance Highway Infrastructure	73
Appendix V	Comments from the Department of Homeland Security	75

Tables

Table 1: Summary of Federal Risk Assessment Activities for Highway Infrastructure	18
Table 2: Summary of Key Programs and Activities to Enhance Security of Highway Infrastructure	45
Table 3: FEMA Grant Funding for Highway Infrastructure-Related Security Projects, 2004 to 2007	52

Figures

Figure 1: Multiple Stakeholders Involved In Highway Infrastructure Security	11
Figure 2: NIPP Risk Management Framework	16

Abbreviations

9/11 Commission Act	Implementing Recommendations of the 9/11 Commission Act
AASHTO	American Association of State Highway and Transportation Officials
ATSA	Aviation and Transportation Security Act
BEL	Bridge Explosives Loading
BZPP	Buffer Zone Protection Program
CBP	U.S. Customs and Border Protection
CIKR	critical infrastructure and key resources
CIP	Critical Infrastructure Protection
CSR	Corporate Security Review
DHS	Department of Homeland Security
DOD	Department of Defense
DOT	U.S. Department of Transportation
FEMA	Federal Emergency Management Agency
FHWA	Federal Highway Administration
FMCSA	Federal Motor Carrier Safety Administration
GCC	Government Coordinating Council
GPRA	Government Performance and Results Act

HITRAC	Homeland Infrastructure Threat and Risk Analysis Center
HMC	Highway and Motor Carrier Division
HSIN	Homeland Security Information Network
HSPD-7	Homeland Security Presidential Directive-7
HSPD-8	Homeland Security Presidential Directive-8
I&A	Office of Intelligence and Analysis
IP	Office of Infrastructure Protection
ISAC	Information Sharing Analysis Center
LLIS	Lessons Learned Information System
MOU	memorandum of understanding
MSRAM	Maritime Security Risk Analysis Model
NCHRP	National Cooperative Highway Research Programs
NIPP	National Infrastructure Protection Plan
NISAC	National Infrastructure Simulation and Analysis Center
NPPD	National Protection and Programs Directorate
NSTS	National Strategy for Transportation Security
OI	Office of Intelligence
OMB	Office of Management and Budget
PDD-63	Presidential Decision Directive 63
PSA	Protective Security Advisor
S&T Directorate	Directorate for Science and Technology
SAV	Site Assistance Visit
SCC	Highway Sector Coordinating Council
SHIRA	Strategic Homeland Infrastructure Risk Assessment
SSA	Sector-Specific Agency
TPFS	Transportation Pooled Fund Study
TRB	Transportation Research Board
TSA	Transportation Security Administration
TSP	Trucking Security Program
TSSP	Transportation Systems Sector-Specific Plan
U.S. Template	Universal Security Template
USCG	U.S. Coast Guard
VIPR	Visible Intermodal Prevention and Response

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office
Washington, DC 20548

January 30, 2009

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

According to the Federal Highway Administration (FHWA), the nation's highway transportation system includes approximately four million miles of roadways, 600,000 bridges, and 50 tunnels over 500 meters in length. This system supports 86 percent of all personal travel, moves 80 percent of the nation's freight (based on value), and serves as a key component in national defense mobility. The U.S. highway system is particularly vulnerable to potential terrorist attacks because of its openness—vehicles and their operators can move freely and with almost no restrictions, and some bridge and tunnel elements are easily accessible and located in isolated areas making them more challenging to secure. Failure to prepare for a terrorist attack against critical highway infrastructure could, according to security experts, lead to catastrophic loss of life and economic disruption estimated to be in the billions of dollars. Thus, the challenge of effectively securing the nation's highway infrastructure against legitimate threats involves balancing the cost and effectiveness of implementing security measures while not impeding the free flow of people and commerce.

Securing the nation's highway infrastructure system is a responsibility shared by federal, state and local governments, and the private sector. Within the Department of Homeland Security (DHS), the Transportation Security Administration (TSA) has primary responsibility for ensuring the security of highway infrastructure. DHS's Infrastructure Protection (IP) Office, whose mission includes leading the coordinated national effort to reduce the risk to critical infrastructure and key resources posed by acts of terrorism, supports TSA's efforts to protect highway infrastructure.¹ In

¹ IP is an organizational entity within the National Protection and Programs Directorate. Critical infrastructure are systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters. Key resources are publicly or privately controlled resources essential to minimal operations of the economy and government. For purposes of this report, we will use the term critical infrastructure to also include key resources.

addition, the U.S. Coast Guard (USCG) is the lead federal agency responsible for the security of the nation's ports and waterways, which may include highway assets that have a maritime nexus, such as bridges. In conjunction with highway infrastructure stakeholders, such as state and local governments, the federal government is involved in a range of security efforts, including conducting risk assessments, providing guidance and training to asset owners, and conducting research and development activities, among others. The federal government is also responsible for providing some funding assistance to highway infrastructure stakeholders. However, the bulk of the responsibility for implementing specific security measures falls largely on state and local governments who own most highway infrastructure, although independent entities, such as public authorities and private entities, own a limited number of major, iconic structures.

You asked us to assess the progress DHS has made in securing the nation's highway infrastructure. This report answers the following questions:

- To what extent have federal entities assessed the risks to the nation's highway infrastructure and coordinated these efforts?
- To what extent has DHS developed a risk-based strategy, consistent with applicable federal guidance and characteristics of an effective national strategy, to guide its highway infrastructure security efforts?
- What actions have government and highway sector stakeholders taken to secure highway infrastructure, and to what extent has DHS monitored the implementation of asset-specific protective security measures?

To identify what efforts federal entities have taken to assess the risk to highway infrastructure and coordinated their efforts, we obtained and analyzed risk assessment data from DHS and the Department of Transportation (DOT), comprised of various threat, vulnerability, and consequence related assessments for highway infrastructure assets.² We sought to determine the reliability of these data by, among other things, obtaining information on the processes used for collecting and

² DHS determined that the risk assessment information is "For Official Use Only." As a result, the related data are not contained in this report.

maintaining written data from agency officials. On the basis of our review of the processes used to collect the data, we determined that the data were sufficiently reliable for the purposes of this report. We interviewed DHS, DOT and selected state transportation, homeland security, and law enforcement officials, associations representing highway infrastructure owners and operators, and members of the Highway Government Coordinating Council (GCC) and the Highway Sector Coordinating Council (SCC), to discuss federal risk assessment efforts.³ We also obtained information on federal coordination and collaboration activities from TSA and highway infrastructure stakeholders and compared these efforts to the coordination requirements established in Homeland Security Presidential Directive-7, as well as GAO's recommended practices for effective collaboration.⁴ To assess the extent to which DHS developed a risk-based strategy consistent with applicable federal guidance, including the National Infrastructure Protection Plan (NIPP) and the Transportation Systems Sector-Specific Plan (TSSP) and best practices to guide its highway infrastructure security efforts, we reviewed federal agency reports, guidelines, and infrastructure security studies on risk management sponsored by industry associations. We also interviewed DHS and DOT officials, state, and industry association highway infrastructure representatives regarding their use of risk management principles for protecting highway infrastructure. As the principal strategy for protecting the nation's highway infrastructure, we also analyzed TSA's Highway Modal Annex to determine how it aligned with the requirements set out in Executive Order 13416, Strengthening Surface Transportation

³ The Highway GCC was established in April 2006, and consists of federal stakeholders and state and local officials with sector-specific security responsibilities. The Highway SCC, established in June 2006, consists of private sector organization, owner-operators, and entities with transportation security responsibilities.

⁴ Homeland Security Presidential Directive-7, issued December 17, 2003, establishes a national policy for Federal departments and agencies to identify and prioritize U.S. critical infrastructure and to protect them from terrorist attacks. The Directive identifies key roles and responsibilities of the DHS Secretary and applicable federal agencies, including requirements for coordination of protection efforts among government agencies and with the private sector. GAO, Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies, [GAO-06-15](#) (Washington D.C: October 21, 2005).

Security.⁵ In addition, we assessed the extent to which the Highway Modal Annex contained the desirable characteristics for an effective national strategy that we have previously identified.⁶ To identify the actions taken by government and highway sector stakeholders to enhance the security of highway infrastructure and assess the extent to which DHS through TSA monitored the implementation of asset specific protective security measures implemented by stakeholders, we interviewed DHS, DOT, and the Department of Defense (DOD), and selected state transportation and homeland security officials; associations representing highway infrastructure operators; and the chairpersons of the Highway GCC and SCC. Although the perspectives of the state transportation and homeland security officials we spoke with cannot be generalized across the wider population of highway infrastructure owners and operators, they provided us a broad overview of highway infrastructure asset security. We selected the associations that we spoke with based on input from TSA, FHWA, and industry stakeholders who identified the major associations representing highway infrastructure owners and operators. We also analyzed TSA reviews of security practices at the state level and records of GCC and SCC meetings and stakeholder conferences. In addition, we selected 12 bridges and 1 tunnel to observe security measures implemented since September 11, 2001, and to discuss security-related issues with highway infrastructure owners and operators. We selected these assets based on criteria including location, ownership, and importance or criticality. We also considered input from TSA, DOT, and the American Association of State Highway and Transportation Officials (AASHTO) to help ensure that selected assets represented those that have implemented a range of security measures—from minimal to more robust.⁷ Due to the limited number of assets in our sample, and because the selected assets did not

⁵ Executive Order 13416, issued in December 2005, mandates that an annex shall be completed for each surface transportation mode in support of the Transportation Systems Sector-Specific Plan. The Highway Infrastructure and Motor Carrier modal annex (Highway Modal Annex) was developed to meet this mandate and is intended to meet the minimum content requirements set forth in this Order. Exec. Order No. 13,416, 71 Fed. Reg. 71,033 (Dec. 5, 2006).

⁶ These characteristics were developed after our research found that there were no legislative or executive mandates identifying a uniform set of required or desirable characteristics for national strategies. For a more detailed discussion of these characteristics, see GAO: Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism, [GAO-04-408T](#) (Washington, D.C: Feb. 3, 2004).

⁷ AASHTO represents highway and transportation departments in the 50 states, the District of Columbia, and Puerto Rico.

constitute a representative sample, the results of our observation and analysis cannot be generalized to the universe of highway infrastructure assets. However, our observations provided us with an overview of the kinds of security measures implemented at some critical infrastructure since September 11, 2001 as well as perspectives on issues highway infrastructure owners and operators face. We also compared TSA's actions to obtain data on actions taken by highway infrastructure stakeholders to enhance security and to monitor implementation of those actions with criteria in Standards for Internal Control in the Federal Government.⁸

We conducted this performance audit from May 2007 through January 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. Appendix I provides additional details about our scope and methodology.

Results in Brief

Federal entities have several efforts underway to assess threat, vulnerability, and consequence—the three elements of risk—for highway infrastructure; however, these assessments have not been systematically coordinated among federal partners. DHS entities—including TSA, the DHS Office of Intelligence and Analysis (I&A), and USCG—each conduct efforts to assess the threats posed to highway infrastructure. For example, the threat assessments developed for the highway sector by TSA's Office of Intelligence (OI) include information about general terrorist activity worldwide and provides additional threat and suspicious incident information to key federal and nonfederal highway infrastructure stakeholders as needed. In addition, TSA's OI has also developed likelihood estimates for specific threat scenarios involving highway infrastructure. The threat information contained in these products is used

⁸ GAO, Standards for Internal Control in the Federal Government, [GAO/AIMD-00-21.3.1](#) (Washington, D.C.: Nov. 1, 1999). These standards, issued pursuant to the requirements of the Federal Managers' Financial Integrity Act of 1982 (FMFIA), provide the overall framework for establishing and maintaining internal control in the federal government. Also pursuant to FMFIA, 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.

to identify specific attack scenarios which serve as an input for the other two components of a risk assessment—assessing the potential vulnerabilities to and consequences of an attack on highway assets. Federal entities have several programs underway to assess the vulnerability of highway infrastructure assets; however, the scope and purpose of these individual efforts vary considerably. For example, TSA conducts reviews of security practices at the state level through its Corporate Security Review (CSR) program to develop a baseline assessment of security nationwide. These reviews have been completed in most states to date, as well as on a select number of individual assets. While TSA’s CSR assessments have a wide scope, IP, USCG, and FHWA operate programs that assess the security vulnerabilities of specific highway assets. However, the various assessments conducted to date were not well coordinated among these key federal partners, and the results have not been routinely shared. According to the NIPP, TSA is responsible for, among other things, coordinating and facilitating comprehensive risk assessment programs for the transportation sector. Our previous work has also shown that one of the principal characteristics of effective collaboration among federal agencies is leveraging available resources.⁹ Without coordinating risk assessment activities and sharing the results, federal entities are missing opportunities to leverage resources and facilitate protection efforts for the greatest number of critical assets.

DHS, through TSA, has developed a strategy to guide highway infrastructure security efforts, but the strategy was not fully informed by available risk assessments, as provided for in federal guidance, and lacks key characteristics that we have identified for an effective national strategy. In accordance with Executive Order 13416, in May 2007, TSA issued the Highway Modal Annex, which serves as the principal strategy for implementing key protective programs for securing the nation’s highway infrastructure. While the completion of the Annex is an important first step in guiding national efforts to protect highway infrastructure, it does not fully incorporate existing risk assessment results to inform and prioritize security efforts. Specifically, according to TSA, the Annex incorporates threat assessment results; however, it is not based on vulnerability and consequence information available from completed federal risk assessments as required by the NIPP and the TSSP. Without considering the results of completed vulnerability and consequence assessments, DHS cannot provide reasonable assurance that its strategy is

⁹ See [GAO-06-15](#).

addressing those areas of greatest risks or that its resources are being prioritized and allocated most effectively and efficiently. In addition, we identified areas where the Annex can be strengthened to be more consistent with Executive Order 13416. For example, the Executive Order requires that the Annex define roles and responsibilities of various stakeholders, yet the Annex only identifies a limited number of stakeholders and does not describe their roles and responsibilities. With so many distinct stakeholders, clearly defined roles and responsibilities for protecting highway infrastructure are vital to help ensure that assets are protected. The Annex also lacks characteristics of an effective national strategy—such as the inclusion of performance goals and measures with which to assess the program’s overall progress toward securing highway infrastructure. Without performance measures and an evaluation of the effectiveness of the Annex’s goals and objectives, TSA does not have meaningful information from which to determine whether the strategy is achieving its intended results and to target any needed improvements. According to TSA officials, the Annex was developed under a relatively short timeframe, which limited government and industry stakeholders’ input to support its development, but TSA officials anticipate that future revisions will contain more detailed information.

Federal entities, along with state and industry stakeholders, have various efforts underway to mitigate risks to highway infrastructure; however, TSA lacks a mechanism to monitor the extent to which highway infrastructure owners have implemented voluntary protective security measures. Efforts taken by federal and non-federal stakeholders to secure highway infrastructure include a combination of publications and training for infrastructure owners and operators, research and development activities, and implementation of specific protective measures intended to enhance the security of infrastructure assets. For example, AASHTO, in conjunction with the FHWA and TSA, has developed and issued several key publications to support states’ efforts to identify critical assets, perform risk assessments, and develop potential countermeasures. A combination of federal and state-led research efforts have also served to identify methods to help protect highway infrastructure, such as the development of measures to reduce the vulnerability of flooding in underwater tunnels and potential attacks to bridge support cables. For example, in fiscal year 2008, the Science and Technology (S&T) Directorate, whose responsibilities include advising the Secretary of Homeland Security on research and development efforts, began to evaluate blast effects and mitigation measures for dams, tunnels, and bridges. In addition to these efforts, infrastructure owners and operators implemented a range of voluntary protective security measures, such as

the installation of cameras and fencing to help control access to vulnerable structures. However, while TSA, through its CSR program, has determined that asset owners are implementing protective actions to secure highway infrastructure, the agency does not have a mechanism to monitor the extent to which specific protective security measures have been implemented for the nation's critical highway infrastructure. According to Executive Order 13416, DHS, through TSA, is tasked with assessing the security of each transportation mode and evaluating the effectiveness and efficiency of current federal government surface transportation security initiatives. Lacking a mechanism to monitor the implementation of voluntary protective security measures, and without evaluating the effectiveness and efficiency of these measures, TSA cannot reasonably determine the level of overall security preparedness for highway infrastructure assets deemed nationally critical.

In order to strengthen collaboration between federal stakeholders involved in securing highway infrastructure, we are recommending that DHS establish a mechanism to systematically coordinate risk assessment activities and share the results of these activities among federal stakeholders. In addition, we are recommending that TSA, in consultation with the Highway GCC and the Highway SCC, incorporate the results of completed risk assessments in future revisions of the Highway Modal Annex; provide clarification of federal and non federal roles and responsibilities related to highway infrastructure protection; and establish timeframes for developing performance goals and measures for highway infrastructure security programs, among other things. Finally, we are recommending that TSA develop a mechanism to monitor the implementation of protective security measures for highway infrastructure assets identified as nationally critical.

We provided a draft of this report to DHS for review. In its written comments, DHS concurred with the recommendations. However, DHS stated that TSA officials believe that GAO has misstated a key fact involving TSA's desire and intention to conduct individual vulnerability assessments on critical highway structures. Specifically, TSA noted that the report indicates that TSA has not decided whether to conduct such assessments or determined that they do not need to be done. Furthermore, TSA stated that it intends to conduct individual assessments on all bridge and tunnel properties that TSA has identified as critical beginning in 2009. Throughout this review, TSA officials repeatedly told us that it would utilize primarily a non asset-specific approach to conducting vulnerability assessments of the highway infrastructure sector, through the Corporate Security Review program. TSA did not make us aware of its plans to

conduct individual vulnerability assessments of critical assets until it provided formal written comments on a draft of this report in January, 2009. While we acknowledge TSA's plans to conduct individual vulnerability assessments on all critical highway infrastructure assets, we do not believe the agency's recently reported plans to conduct these assessments affect the findings of this report. Nevertheless, we added a discussion to this report to clarify TSA's plans related to vulnerability assessments.

Background

The nation's highway transportation system includes infrastructure, vehicles and users, equipment, facilities, and control and communications. Infrastructure or the "fixed" aspect of the highway transportation system includes roads, bridges, tunnels, and terminals, where travelers and freight can enter and leave the system. Many vehicle types operate on the highway system, moving both people and freight. Highway system users include commercial vehicle and private passenger drivers, cargo shippers and receivers, passengers, and pedestrians. Equipment refers to items such as machinery, cones, barriers and bollards used to create stand off distance. Facilities include terminals, warehouses, depots, and other transportation-related buildings that support the highway system. Finally, control and communications are methods for controlling vehicles, infrastructure, and the entire transportation network. These items include traffic lights, message signs, call boxes, ramp metering, closed circuit television and speed monitoring systems.

Although these security enhancements are typically funded by the asset owner, the Federal Emergency Management Agency (FEMA) has provided funding to secure highway infrastructure through its grant programs. DHS funding for highway infrastructure security consists of a general appropriation to TSA for its entire surface transportation security program, which includes commercial vehicles and highway infrastructure, rail and mass transit, and pipeline security, and appropriations to FEMA for its Homeland Security Grant Program and Infrastructure Protection Program.¹⁰ Annual appropriations to TSA for its surface transportation security program were \$36 million in fiscal year 2006, \$37.2 million in fiscal

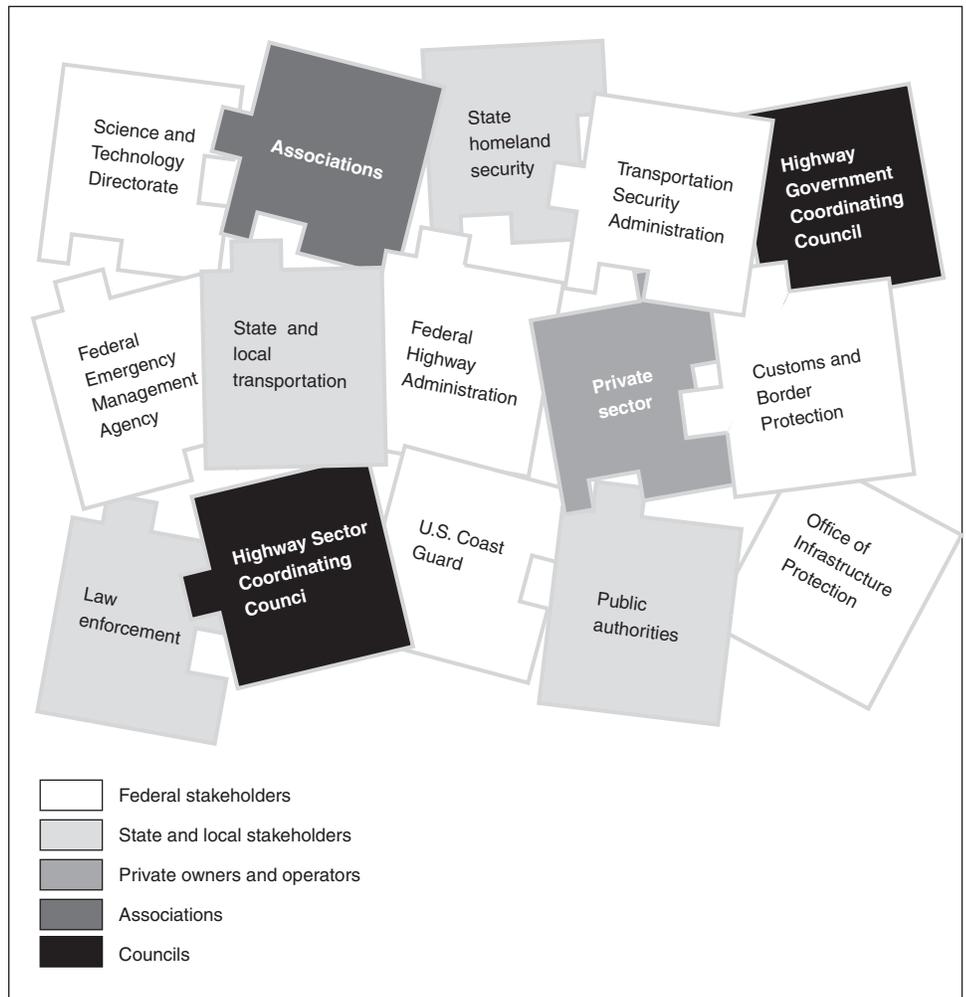
¹⁰ The Homeland Security Grant Program consists of three underlying programs that have been used, in part, to finance highway infrastructure security enhancements—the State Homeland Security Program, the Urban Area Security Initiative, and the Law Enforcement Terrorism Prevention Program. Under the Infrastructure Protection Program, highway infrastructure security efforts have primarily been funded through the Buffer Zone Protection Program (BZPP) and the Trucking Security Program.

year 2007, \$46.6 million in fiscal year 2008, and \$49.6 million in fiscal year 2009. Total FEMA funding available under the two principal grant programs increased from approximately \$2 billion to over \$2.5 billion from fiscal years 2006 through 2008.

Multiple Stakeholders Share Responsibility for Securing Highway Infrastructure

Protecting the nation's highway infrastructure can be complicated due to the number of stakeholders involved. As illustrated in figure 1, numerous entities at the federal, state, and local levels, including public and private sector owners and operators, play a key role in highway infrastructure security. Highway infrastructure in the United States is owned and operated by a combination of federal entities, states, counties, municipalities, tribal authorities, private enterprise, and groupings of these entities. Although state and local governments own, operate, and have law enforcement jurisdiction over most of the highway infrastructure in the United States, bridge and turnpike authorities operate some major infrastructure, and there are a few privately owned bridges, tunnels, and roadways.

Figure 1: Multiple Stakeholders Involved In Highway Infrastructure Security



Source: GAO analysis.

DHS is the cabinet level department with primary responsibility for helping to secure highway infrastructure.¹¹ Within DHS, TSA has primary responsibility for securing all modes of transportation, including highway

¹¹ Prior to the terrorist attacks of September 11, 2001, DOT was the primary federal entity involved in regulating highway infrastructure as it concerned safety. No particular entity was responsible for highway infrastructure security prior to the establishment of TSA.

infrastructure with support from other DHS entities including the National Protection and Programs Directorate (NPPD), USCG, Science and Technology Directorate, FEMA, and U.S. Customs and Border Protection (CBP). For example, as part of its mission, CBP is responsible for preventing people or goods that could threaten infrastructure from entering ports of entry. Although TSA is the lead agency responsible for the security of highway infrastructure, DOT, through FHWA, provides highway transportation expertise to assist TSA with respect to securing highway infrastructure.¹²

NPPD, through IP, is responsible for coordinating efforts to protect the nation's most critical assets across all critical infrastructure and key resources, which includes surface transportation. Within the transportation sector, IP works with TSA to identify nationally critical highway assets. USCG also conducts activities in support of highway infrastructure protection, such as identifying potential vulnerabilities of individual highway assets that have a maritime nexus or that affect the marine transportation system, such as bridges over navigable waterways. The Science and Technology Directorate is responsible for advising the Secretary on research and development efforts to support the Department's mission and conducts research to identify and mitigate vulnerabilities to bridges and tunnels. FEMA is responsible for awarding and administering DHS grant funds in conjunction with responsible program offices. While federal stakeholders play a role in facilitating risk-based infrastructure security efforts, implementation of asset-specific protective security measures remains the responsibility of individual asset owners-operators, most commonly states or other public entities.

A number of national organizations and coordination groups exist to represent the broad composition of public and private sector highway infrastructure stakeholders. At the state level, representation is provided by AASHTO. To date, AASHTO has played a key role in representing state interests related to protecting highway infrastructure and routinely collaborates with federal entities to assist their members in enhancing infrastructure security. In April 2006, the Highway GCC was established to foster communication across government agency lines, and between the government and private industry, in support of the nation's homeland

¹² Homeland Security Presidential Directive-7 (HSPD-7) directed DOT and the DHS to collaborate on all matters related to transportation security and transportation infrastructure protection.

security mission. The Highway GCC membership largely consists of key Federal departments and stakeholders responsible for or involved with highway and motor carrier security, but also includes key entities such as AASHTO. The objective of the Highway GCC is to coordinate highway and motor carrier security strategies and activities; establish policies, guidelines and standards; and develop program metrics and performance criteria for the highway mode. The counterpart to the Highway GCC is the Highway SCC. This group is comprised of private sector owners and operators and representative associations of highway and motor carrier assets. The Highway SCC is an industry advisory body that, as appropriate, is to coordinate the private industry perspective on highway and motor carrier security policy, practices, and standards that affect the highway mode.

Laws and Federal Guidance Concerning the Security of Highway Infrastructure

Federal laws and directives call for critical infrastructure protection activities to help secure infrastructure assets that are essential to national security. While a number of federal laws impose safety requirements on highway infrastructure, no federal laws explicitly require highway infrastructure operators to take action to safeguard their assets against a terrorist attack. In November 2001, the Aviation and Transportation Security Act (ATSA) generally required TSA to (1) receive, assess, and distribute intelligence information related to transportation security; (2) assess threats to transportation security and develop policies, strategies, and plans for dealing with those threats, including coordinating countermeasures with other federal organizations; and, (3) enforce security-related regulations and requirements.¹³ Further, in November 2002, the Homeland Security Act of 2002 created DHS and mandated IP to comprehensively assess the vulnerabilities of the critical infrastructure and key resources of the United States; integrate relevant information, intelligence analyses, and vulnerability assessments to identify protective priorities and support implemented protective security measures; and develop a comprehensive national plan for securing the key resources and critical infrastructures of the United States.¹⁴ The Intelligence Reform and Terrorism Prevention Act of 2004 also requires DHS to develop and implement a National Strategy for Transportation Security to include an identification and evaluation of the transportation assets that must be protected from attack or disruption, the development of risk-based

¹³ Pub. L. No. 107-71, § 101(a), 115 Stat. 597, 598 (2001) (codified at 49 U.S.C. § 114(f)).

¹⁴ Pub. L. No. 107-296, §§ 101, 201(d), 116 Stat. 2135, 2142, 2145-46 (2002).

priorities for addressing security needs associated with such assets, means of defending such assets, a strategic plan that delineates the roles and missions of various stakeholders, a comprehensive delineation of response and recovery responsibilities, and a prioritization of research and development objectives.¹⁵ More recently, in August 2007, the Implementing Recommendations of the 9/11 Commission Act (9/11 Commission Act), among other things, specified that the transportation modal security plans, including the plan for highways, required by the Intelligence Reform and Terrorism Prevention Act must include threats, vulnerabilities, and consequences, and requires DHS to establish a Transportation Security Information Sharing Plan.¹⁶

The President has also issued directives concerning protecting critical infrastructure. In May 1998, Presidential Decision Directive 63 (PDD-63) established critical infrastructure protection as a national goal and presented a strategy for cooperative efforts by the government and infrastructure stakeholders to protect the physical and cyber-based systems essential to the minimum operations of the economy and the government. In addition, in December 2003, HSPD-7 was issued, superseding PDD-63. HSPD-7 defines responsibilities for DHS, federal stakeholders that are responsible for addressing specific critical infrastructure sectors—sector-specific agencies, and other departments and stakeholders. HSPD-7 instructs these sector-specific agencies to collaborate with all relevant Federal departments and agencies, State and local governments, and the private sector, including with key persons and entities in their infrastructure sector; conduct or facilitate vulnerability assessments of the sector; and encourage risk management strategies to protect against and mitigate the effects of attacks against critical infrastructure and key resources. HSPD-7 designates DHS as responsible for, among other things, coordinating national critical infrastructure protection efforts and establishing uniform policies, approaches, guidelines, and methodologies for integrating federal infrastructure protection and risk management activities within and across sectors. Moreover, Homeland Security Presidential Directive-8 (HSPD-8), issued at the same time as HSPD-7, directs DHS to coordinate the development of an all-hazards National Preparedness Goal that establishes measurable

¹⁵ Pub. L. No. 108-458, § 4001(a), 118 Stat. 3638, 3710 (2004) (codified as amended at 49 U.S.C. § 114(s)).

¹⁶ Pub. L. No. 110-53, §§ 1202, 1203, 121 Stat. 266, 381-86 (2007). At the time of our review, DHS had not issued this plan.

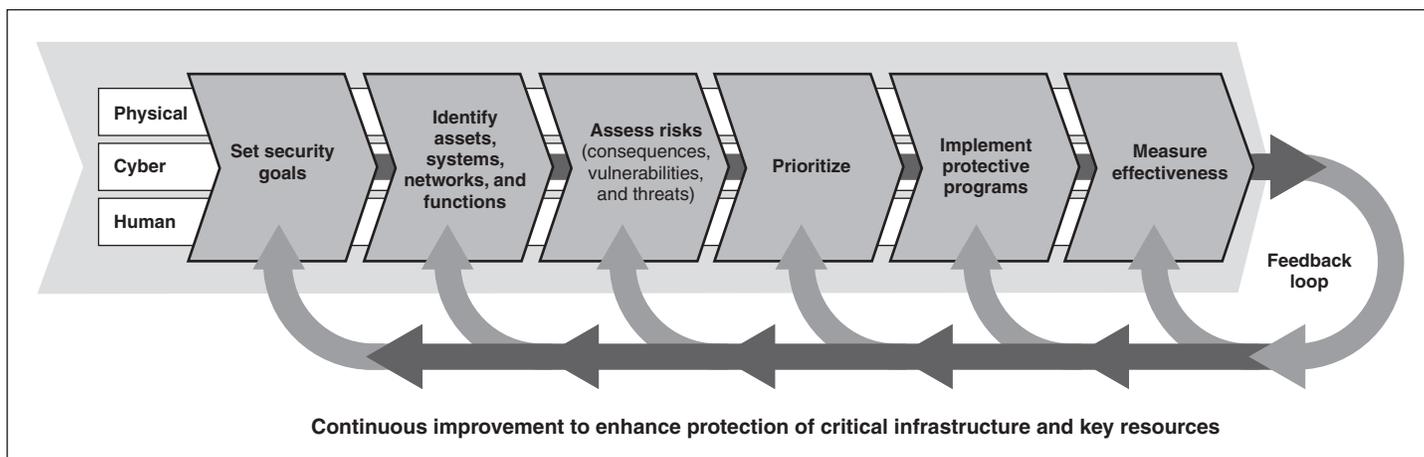
priorities, targets, standards for preparedness assessments and strategies, and a system for assessing the Nation's overall level of preparedness. Further, in December 2006 the President issued Executive Order 13416, which focused on strengthening the security of surface transportation modes and requires DHS to assess the security of each surface transportation mode and evaluate the effectiveness and efficiency of current surface transportation security initiatives.¹⁷ For additional key federal laws and guidance related to critical highway infrastructure protection, see Appendix II.

Risk Management Approach to Guide Homeland Security Investments

Recognizing that each sector possesses its own unique characteristics and risk landscape, HSPD-7 designates Federal Government Sector Specific Agencies (SSAs) for each of the critical infrastructure sectors who are to work with DHS to improve critical infrastructure security. On June 30, 2006, DHS released the NIPP, which developed—in accordance with HSPD-7—a risk-based framework for the development of Sector-Specific Agency (SSA) strategic plans. The NIPP defines roles and responsibilities for security partners in carrying out critical infrastructure and key resources (CIKR) protection activities through the application of risk management principles. Figure 2 illustrates the several interrelated activities of the risk management framework as defined by the NIPP, including setting security goals and performance targets, identifying key assets and sector information, and assessing risk information including both general and specific threat information, potential vulnerabilities, and the potential consequences of a successful terrorist attack. The NIPP requires that federal agencies use this information to inform the selection of risk-based priorities and for the continuous improvement of security strategies and programs to protect people and critical infrastructure through the reduction of risks from acts of terrorism.

¹⁷ Exec. Order No. 13,416, 71 Fed. Reg. 71,033 (Dec. 5, 2006).

Figure 2: NIPP Risk Management Framework



Source: DHS.

The NIPP risk management framework consists of the following interrelated activities:

- **Set security goals:** Define specific outcomes, conditions, end points, or performance targets that collectively constitute an effective protective posture.
- **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.
- **Assess risks:** Determine risk by combining 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), known vulnerabilities to various potential attack vectors, and general or specific threat information.
- **Prioritize:** Aggregate and analyze risk assessment results to develop a comprehensive picture of asset, system, and network risk; establish priorities based on risk; and determine protection and business continuity initiatives that provide the greatest mitigation of risk.
- **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.

-
- **Measure effectiveness:** Use metrics and other evaluation procedures at the national and sector levels to measure progress and assess the effectiveness of the national Critical Infrastructure and Key Resources protection program in improving protection, managing risk, and increasing resiliency.

Federal Entities Have Initiated Efforts to Assess Risks to Highway Infrastructure, But Coordination of These Efforts is Limited

Several federal entities have efforts underway to assess threat, vulnerability, and consequence—the three elements of risk—for highway infrastructure; however, these assessments have not been systematically coordinated among key federal partners. DHS agencies and offices, including TSA, I&A, and USCG, each have efforts underway to assess the threats posed to highway infrastructure, including the most likely tactics that terrorists may use and potential targets. Federal agencies are also assessing the security vulnerabilities of and consequences of an attack on highway assets to some degree, although the scope and purpose of these individual efforts vary considerably. However, the risk assessment activities conducted to date have not been systematically coordinated among the federal partners. Given competing departmental priorities and limited resources identified by TSA and IP officials, it is important for federal stakeholders to coordinate their efforts and share available risk information to avoid potential duplication, better focus future assessment efforts, and leverage limited resources.

Federal Stakeholders Have Taken Actions to Assess Risks to Highway Infrastructure

Several DHS stakeholders play a role in securing highway infrastructure, including TSA, I&A, IP, and USCG—along with FHWA within DOT. Collectively, they have a number of independent efforts underway to conduct threat, vulnerability, and consequence assessments of highway assets. Although the scope and purpose of these individual efforts vary by entity and are at various levels of completion, they have been used to a limited extent to assess the general state of security for the sector, and to identify potential security enhancements for a majority of highway infrastructure assets identified as nationally critical. See table 1 for a summary of federal risk assessment activities related to highway infrastructure assets.

Table 1: Summary of Federal Risk Assessment Activities for Highway Infrastructure

Agency/ Office	Program/ Activity	Description	Risk Component		
			Threat	Vulnerability	Consequence
Transportation Security Administration (TSA)					
Office of Intelligence	Highway Threat Assessments	Provides an overview of threats—including key actors and possible attack tactics and targets—to the National Highway System and its critical infrastructure. Includes incidents of interest and suspicious activity targeting various highway modes (e.g. bridges, tunnels) in the United States and overseas.	X		
Highway and Motor Carrier Division (HMC)	Corporate Security Reviews (CSRs)	TSA conducts CSRs with state DOTs to establish baseline data to assess the state of security nationwide and identify common practices used to secure highway infrastructure. In conjunction with the State CSRs, HMC has also conducted a limited number of asset-specific CSRs.		X	
Office of Infrastructure Protection (IP) / DHS Office of Intelligence and Analysis (I&A)					
Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) ^a	Strategic Homeland Infrastructure Risk Assessment (SHIRA)	Provides a national overview of current high-risk scenarios for critical infrastructure across all industry sectors, including attacks on select highway infrastructure. Scenarios are identified on the basis of available threat information, perceived vulnerabilities of the sector, and the potential consequences of a successful attack.	X	X	X

Agency/ Office	Program/ Activity	Description	Risk Component		
			Threat	Vulnerability	Consequence
Office of Infrastructure Protection	Site Assistance Visits (SAVs) & Buffer Zone Protection Program (BZPP)	<p>These programs are intended to provide DHS and applicable stakeholders with detailed information about asset vulnerabilities to help it identify potential mitigation efforts and reduce potential consequences of an attack.</p> <ul style="list-style-type: none"> SAV: Facility-level assessments conducted by a federally-led team in partnership with asset owners. Mitigation measures to address identified vulnerabilities are provided to owners as “options for consideration.” BZPP: An assessment conducted by local law enforcement of the “buffer area” in the vicinity of critical infrastructure which may be used to conduct surveillance or an attack. The results are utilized to identify resource needs and develop a purchasing plan, funded through a DHS grant program, to reduce vulnerabilities and mitigate potential consequences. 		X	X
Office of Infrastructure Protection	Tier 1/Tier 2 Program ^b	In conjunction with SSAs and state Homeland Security Advisors, this effort identifies nationally significant, high-consequence assets and systems that, if destroyed or disrupted, could cause significant casualties, major economic losses, or widespread and long-term disruptions to national well-being and governance capacity. The Tier 2 CIKR assets include nationally-significant and high-consequence assets. Tier 1 assets are a small subset of the Tier 2 list that include assets and systems certain to produce the most significant consequences.			X
U.S. Coast Guard (USCG)					
Port Security Specialists	Maritime Security Risk Analysis Model (MSRAM)	USCG conducts assessments on key maritime bridges and tunnels with a maritime nexus, as part of its annual risk assessment of each port, via the MSRAM.	X	X	X

Agency/ Office	Program/ Activity	Description	Risk Component		
			Threat	Vulnerability	Consequence
Port Security Assessment Teams	Terrorist Operations Assessments	From 2004 through 2005, USCG also conducted port-wide vulnerability assessments at several of the nation's most critical ports. These assessments, in part, targeted key bridges and tunnels that had not undergone any other federal assessments.		X	
Federal Highway Administration (FHWA)					
Office of Infrastructure	Vulnerability Assessments	FHWA conducts vulnerability assessments and provides subject matter expertise and technical assistance upon request to DHS/TSA; state, local, and tribal governments; private sector stakeholders; and infrastructure owners.		X	

Source: GAO analysis.

^aHITRAC represents a joint effort between IP and the Critical Infrastructure Threat Analysis Division within I&A.

^bAssets identified as nationally significant through this program are placed into two distinct tiers based on the estimated consequences to the nation.

Threat Assessments

DHS stakeholders develop a combination of products that identify what they have determined to be the most probable threat scenarios involving highway infrastructure. For example, TSA's OI issues an annual threat assessment of the U.S. highway system and provides additional threat and suspicious incident information to key federal and nonfederal highway infrastructure stakeholders as needed.¹⁸ Recent suspicious activity involving highway infrastructure reported by the media could suggest potential terrorist plans to attack the nation's highway system. For example, in July 2008, the media reported a U.S.-educated female Pakistani neuroscientist suspected of having links to Al Qaeda, while captured in Afghanistan, was found carrying handwritten notes referring to a "mass casualty attack" on famous locations in New York, including the Brooklyn Bridge.¹⁹ In addition to the issuance of the Highway Threat Assessment, TSA's OI has also developed likelihood estimates for specific threat scenarios involving highway infrastructure. These estimates include scores of both terrorist intent and capability—the key components of threat—for

¹⁸ Specific threat information is "For Official Use Only" and is not contained in this report.

¹⁹ According to TSA officials, investigation of this incident was still ongoing and no additional details were provided.

five specific threat scenarios. These scores are intended to serve as the input for the threat component of the overall risk equation that TSA uses: Risk = f(Threat x Vulnerability x Consequences).

The Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), which is a joint program office between the Office of Infrastructure Protection and the Office of Intelligence and Analysis, manages the Strategic Homeland Infrastructure Risk Assessment process. The results of this process provide a national overview of current high-risk scenarios for all critical infrastructure and key resources, which includes attacks on select highway infrastructure. In developing these scenarios, analysts consider terrorist capability and intent (threat), as well as vulnerability and consequence information.²⁰ While this product is not intended to cover the full range of potential threat scenarios posed to the highway sector, it may serve to assist TSA and other federal highway security stakeholders in identifying specific high-risk scenarios that may require additional focus or resources.

As part of its annual risk assessment of maritime infrastructure, USCG has also developed a number of threat scenarios involving select bridges and tunnels. USCG uses threat information provided internally by its Intelligence Coordination Center to evaluate 19 different attack scenarios for each infrastructure asset via the Maritime Security Risk Analysis Model (MSRAM).²¹ As with TSA and IP, USCG uses threat information as an input when conducting assessments of potential vulnerabilities and consequences of an attack on maritime highway infrastructure.

Vulnerability Assessments

According to the NIPP, DHS is responsible for ensuring that comprehensive vulnerability assessments are performed for infrastructure that is deemed nationally critical. Given the potential for loss of life, economic disruption, and other impacts resulting from an attack on critical highway infrastructure, DHS stakeholders and other federal partners have a number of efforts underway to assess the vulnerabilities of these assets. These efforts are intended to help identify potential security gaps and prioritize mitigation solutions. However, the degree to which

²⁰ As part of the analysis conducted to determine the high-risk scenarios identified in the SHIRA report for the highway sector, IP incorporated vulnerability and consequence data provided by TSA, as well as input from DOT.

²¹ MSRAM is a terrorism risk analysis tool used by USCG units to identify critical infrastructure and support risk-based security decisions.

vulnerability assessments have been completed for individual highway infrastructure assets varies considerably between these entities, given their available resources and other security priorities. For example, given the substantial number of highway infrastructure assets under their jurisdiction and staffing limitations, TSA's Highway Motor Carrier Division (HMC) has chosen to identify highway infrastructure vulnerabilities by working primarily with State departments of transportation to identify the extent to which common security practices are employed.²² However, more comprehensive asset-specific vulnerability analyses are conducted by both IP and USCG, although the scope and purpose of the resulting products vary considerably. While these distinct entities each have vulnerability assessment efforts underway, the assessment efforts of TSA and IP have slowed considerably due to other identified priorities, and no timeframes currently exist for their completion. In addition, during the course of this review TSA officials stated TSA, as the Sector-Specific Agency for highway infrastructure, had not yet determined whether asset-specific federal vulnerability assessments should be completed for all critical highway infrastructure. However, when providing written comments on this report in January 2009, TSA officials noted that they intend to conduct individual assessments on all bridge and tunnel properties that it has identified as critical beginning in 2009. The following represents the specific vulnerability assessment activities conducted by DHS entities and their federal partners.

TSA – Highway Motor Carrier Division

Through its CSR program, HMC conducts interviews with state officials to assess the security plans, policies, and security actions of organizations whose operations include critical highway infrastructure. As part of these interviews, TSA utilizes standardized questions to document the extent to which security efforts have been implemented within 11 functional areas, including security planning, physical security measures, and security training programs, among others.²³ These security reviews focus primarily on state DOT offices, but may include other state agencies with transportation security functions, such as the Offices of Emergency

²² The HMC division of TSA currently has 19 staff and is responsible for managing the following functional areas: Trucking and Hazardous Materials, Motor coaches, School Transportation, Commercial Drivers Licenses, and Highway Infrastructure.

²³ The 11 CSR functional areas identified by TSA include: threat assessments, vulnerability assessments, security planning, credentialing, designation and management of secure areas, critical asset identification, physical security measures, cyber security measures, security training, communications practices, and security exercises.

Management or Homeland Security. At the time of our review, HMC officials stated that the resources associated with conducting vulnerability assessments makes it impractical to conduct asset-specific assessments of the vast number of bridges and tunnels that comprise the nation's highway system. For this reason, HMC had chosen to utilize primarily a non asset-specific approach to conducting vulnerability assessments of the highway infrastructure sector, through the CSRs. HMC officials stated that they rely on infrastructure owners and operators to conduct asset-level vulnerability assessments on highway assets, and that they generally review these findings as a component of their CSR activities. However, as previously stated, after reviewing a draft this report, TSA commented in January 2009 that it intends to conduct individual assessments on all bridge and tunnel properties that TSA has identified as critical beginning in 2009.

Since the CSR program was initiated in May 2004, HMC has completed CSRs for most of the states and a select number of CSRs for specific highway infrastructure assets.²⁴ According to HMC officials, the goal of these efforts is to assess potential security gaps and provide state officials with suggested actions for strengthening security. However, the pace of TSA's CSR program has slowed considerably in recent years, and no timeframe currently exists for their completion for all 50 states. Specifically, most of the state level CSRs were conducted during the first two years of the program's implementation, which began in May 2004. HMC officials stated that a combination of competing priorities and a reduction in staff available to perform CSR's led to the slowing of this effort. Specifically, HMC officials said that the 9/11 Commission Act placed a number of additional requirements on the division, such as completing a national risk assessment for school buses. While HMC officials are currently planning to conduct highway infrastructure CSR's in all remaining states, it remains unclear if, or when, this will be achieved.²⁵ In accordance with standard program management principles, timeframes or milestones should typically be incorporated as part of a road map to

²⁴ While HMC has identified these visits as asset-specific CSRs, HMC documented its findings for a limited number of cases. The other visits did not result in a formal CSR report.

²⁵ According to HMC officials, the decision to complete CSR's in all 50 states was largely attributable to a request by AASHTO. Prior to this decision, HMC documented that CSR's would be conducted on the basis of risk and prioritized to those states with greater numbers of critical highway infrastructure assets.

achieve a specific desired outcome or result.²⁶ The voluntary nature of the CSR program contributes to the inability for TSA to establish clear timeframes for completion. For example, according to HMC officials, two states have already declined to participate in the CSR program due to their lack of perceived security risk to their assets. In January 2009, HMC officials said that one of those states subsequently reversed its decision and is willing to participate in the CSR program. In 2008, HMC also began conducting follow-up state level CSR's to states previously assessed, and has completed a limited number of such assessments as of January 2009. According to TSA officials, the purpose of these visits is to update existing data and determine current infrastructure security efforts at the state-level.

In the absence of CSR vulnerability data for infrastructure assets in the remaining states, TSA may rely on other mechanisms to obtain this data. As outlined in HSPD-7, the SSA is responsible for conducting or facilitating vulnerability assessments across the sector. According to TSA officials, the CSR effort represents their primary mechanism for meeting this responsibility. Yet, given competing priorities and resource limitations identified by HMC, there may be limited value to expending further resources to complete highway infrastructure CSRs in states or territories lacking any critical assets. Specifically, only two remaining states or territories that have not undergone a CSR have any highway infrastructure assets deemed nationally critical by IP. However, to obtain vulnerability information for the remaining critical assets, TSA could conduct a CSR visit or collaborate with other highway sector stakeholders. For example, HMC may be able to leverage the resources of other federal partners that have completed vulnerability assessments for those assets. Another potential option includes the utilization of the existing bridge safety program to obtain information about critical asset vulnerabilities. According to HMC officials, they are currently conducting pilot programs with several states to incorporate security-related questions within mandatory National Bridge Inspection program conducted biennially by state inspectors.²⁷ While TSA has stated that it intends to conduct individual assessments on all bridge and tunnel properties that it has identified as critical, TSA does not plan to begin those assessments until

²⁶ The Standard for Program Management© (The Project Management Institute, 2006).

²⁷ According to HMC officials, the effort has the full support of AASHTO but remains dependent on individual states to support additional training and other requirements related to these efforts.

our review is completed. Thus, it is too early to tell whether these assessments will provide TSA with sufficient data about asset vulnerabilities to make informed decisions about sector needs and priorities.

Office of Infrastructure Protection (IP)

As part of its responsibility to help protect critical infrastructure in all industry sectors, since 2002, IP has completed a number of vulnerability assessments of specific highway infrastructure assets through two key programs.²⁸ Specifically, IP has conducted, or participated in, assessments evaluating vulnerabilities of major roadways, bridges, and tunnels as part of its SAV and BZPP programs. While the scope and purpose of these two programs differ considerably, they each serve to provide DHS, as well as applicable stakeholders and owners and operators, with detailed information about identified asset vulnerabilities to develop and prioritize mitigation efforts.

Site Assistance Visits (SAVs). This voluntary program includes asset-level vulnerability assessments conducted by a federally-led team in partnership with asset owners and operators. SAVs are designed to facilitate discussion about vulnerability identification and mitigation between security partners and asset owners and operators. The visits, which take between one and three days to complete, incorporate various attack scenarios to identify potential asset vulnerabilities that could be exploited by a potential terrorist. Given the voluntary nature of the SAVs, implementation of identified mitigation measures is not required through the program; however, IP provides asset owners and operators with “options for consideration” intended to help them detect and prevent terrorist attacks. According to IP officials, their experience has shown that asset operators are generally willing to address these options because it is in their best economic and social interest to do so, given the potential consequences that may result in the event of an attack. As of January 2009, IP has conducted SAVs on a number of highway infrastructure assets; however, many of these were completed prior to July 2005.

Buffer Zone Protection Program (BZPP). Under this DHS grant program, IP assists state and local authorities, as well as private industry, in developing protection plans for critical infrastructure assets, including

²⁸ The number of vulnerability assessments that were conducted is designated “For Official Use Only” and is not contained in this report.

selected highway assets. Unlike the SAV, which focuses on the security of infrastructure assets directly, the BZPP focuses on the buffer area surrounding an asset that a terrorist may use to conduct surveillance or an attack. While DHS provides the assessment tools as well as operational and technical support, the actual BZPP assessment is conducted by local law enforcement agencies with jurisdiction over the selected asset. Based on the vulnerabilities identified during the assessment, a Buffer Zone Plan is developed, in cooperation between IP and state and local partners, to address potential security gaps and identify measures to deter terrorist activity near key assets. As part of this plan, recommended enhancements are identified that may be eligible for grant funding based on a validation of the assessment and approval of a spending plan by IP officials.²⁹ Potential items funded through this program include personal protective equipment, interoperable communication equipment, patrol boats, and detection equipment, among others. Since October 2002, a number of highway infrastructure assets have been assessed through the BZPP program, and additional highway assets were assessed since fiscal year 2006.³⁰

While BZPP and SAV assessments serve as some of DHS' principal efforts to identify vulnerabilities and inform risk analysis of the highway sector, the pace of both of these activities has slowed considerably since 2006 due, in large part, to competing agency priorities. According to IP officials, the principal reason for the reduction in these activities is the office's focus on sectors that are a higher priority, such as dams and nuclear facilities. Since 2006, these sectors have been deemed a higher priority due to the potential for catastrophic effects resulting from a terrorist attack. Moreover, it is uncertain to what extent IP vulnerability assessments will be conducted on additional highway infrastructure assets in the future because no timeframes for additional assessments currently exist and future resource priorities remain unknown.

**United States Coast Guard
(USCG)**

As part of its maritime security responsibilities, USCG completes an annual risk assessment of all key bridges and tunnels that are located on

²⁹ Requests for federal funding under the BZPP are tracked using the Vulnerability Reduction Purchasing Plan. Once the plan is reviewed and approved by IP, FEMA is responsible for administering the funds and monitoring expenditures.

³⁰ Grant funding available through the BZPP program was approximately \$91 million in 2005 and approximately \$50 million for each fiscal year from 2006 through 2008.

or within U.S. navigable waters. In addition to this broad effort, USCG has also conducted more comprehensive vulnerability assessments for a number of critical maritime bridges and tunnels as part of its Terrorist Operations Assessments completed in the wake of the attacks on September 11, 2001.

Maritime Security Risk Analysis Model (MSRAM). Each year, USCG uses the MSRAM to develop a risk-score for maritime infrastructure likely to result in significant potential consequences if attacked, including select bridges and tunnels, as part of its port-wide risk assessments. The vulnerability component of the model is determined by identifying any applicable protective measures employed, such as access controls, perimeter security and surveillance, and explosives detection, among others, against a number of identified threat scenarios. According to USCG officials, all available federal assessments, such as SAVs, as well as those conducted by private contractors, are incorporated into the analysis to assist in determining the vulnerability of each asset being assessed. The purpose of the model is to identify port critical infrastructure that may pose the highest overall risk. The resulting information is then used to prioritize USCG security efforts and guide security planning actions with maritime stakeholders.³¹ USCG does not regulate or enforce the risk mitigation efforts for bridges and tunnels. According to USCG officials, these efforts remain voluntary and it is the owner or operator's responsibility to implement potential countermeasures. The MSRAM tool currently covers approximately 370 maritime bridges and tunnels, including the majority of critical highway assets identified by DHS in 2007.

Terrorist Operations Assessments. USCG also performed vulnerability analyses on a number of maritime bridges and tunnels as a component of port-wide security assessments conducted at the nation's most critical ports after the attacks of September 11, 2001. These vulnerability assessments were conducted on a number of individual bridges and tunnels selected based on a combination of their perceived criticality and the absence of any previous federal assessments conducted. According to USCG officials, these assessments helped inform the agency's infrastructure security operations and were incorporated into the MSRAM analysis described above. The results of these assessments were also

³¹ Stakeholder security efforts are coordinated within the Area Maritime Security Committee, whose members may include asset owners and operators of maritime bridges and tunnels.

shared with the owners and operators of the assets, according to USCG officials.

Federal Highway Administration (FHWA)

Although DHS entities are currently the primary lead for federal highway infrastructure risk assessments, FHWA has played a key role in facilitating these efforts. Beginning in 2003, FHWA began conducting risk management workshops and responded to requests by state officials to conduct vulnerability assessments of selected bridges and tunnels that the states had identified as critical. To date, FHWA has taken the lead for conducting assessments at the state or local-level, as well as additional asset-specific assessments. Collectively, these assessments cover a number of individual bridges and tunnels, including some identified as critical assets. According to FHWA, owners generally receive a report of all assessment findings, including a suite of measures that can be used to make a facility more secure. However, officials noted that it remains the decision of the asset owner to determine how much risk to accept and how much money should be invested to protect against terrorism. From 2004 through 2005, FHWA also played a key role in assisting USCG conduct its port-wide vulnerability assessments. According to FHWA officials, their current role is to help support DHS' overall efforts to protect highway infrastructure by providing subject matter expertise; participating in assessments with various DHS entities; conducting training, and developing guidance, in conjunction with AASHTO, to assist states in conducting their own risk assessments of transportation infrastructure.

Consequence Assessments

Although federal entities have collected consequence information as part of their ongoing efforts to identify critical assets and conduct vulnerability assessments, detailed consequence assessments of highway infrastructure have been limited. According to the NIPP, risk assessments should include consequence assessments to measure key effects to the well being of the nation. These effects include the negative consequences on public health and safety, the economy, public confidence in national economic and political institutions, and the functioning of government that can be expected if an asset, system, or network is damaged, destroyed, or disrupted by a terrorist attack.

On a sector-wide basis, TSA and IP work together to develop a list of highway infrastructure assets deemed nationally critical based on several

consequence-related factors, such as the potential loss of life and economic impact.³² While this list is not intended to provide the type of detailed consequence information used to prioritize mitigation decisions between specific assets, as called for in the NIPP, DHS officials stated that it serves to identify those assets that should be considered when conducting more comprehensive risk assessments of the sector. Since 2007, IP has been responsible for developing critical asset lists for all critical infrastructure and key resources in conjunction with applicable SSAs and state and territorial Homeland Security Advisors. This list is broken into two distinct tiers based on estimated consequences to the nation. The first list, Tier 1, is comprised of critical infrastructure assets and key resources that, if disrupted or destroyed, would have significant negative consequences. Currently, no highway infrastructure assets are included on the Tier 1 list. The Tier 2 list includes highway infrastructure that, based on established criteria, represent assets that, if destroyed, are also likely to result in relatively significant potential negative consequences to the nation.

As part of DHS's effort to assess risk to the nation's critical infrastructure, HITRAC also engages in a collaborative effort with SSAs to collect consequence information. Specifically, HITRAC incorporates analysis of potential consequences when developing the high-risk threat scenarios contained within the SHIRA report. For example, HITRAC disseminates worksheets to each of the SSA's to collect estimates of consequences resulting from a variety of different attack scenarios. For each scenario, the SSA develops numerical rankings for several categories of potential consequences, including potential loss of life, economic effects, psychological consequences, and potential effect on agency mission. Upon review of this data, HITRAC is then able to identify and prioritize those scenarios that are likely to result in significant potential consequences relative to other attack methods or targets. In addition, some asset-level federal vulnerability assessments, such as SAVs, also include estimates of potential consequences. For example, the standard template used to record information during these visits incorporates a series of questions regarding consequences to estimate the potential loss of life and other economic consequences resulting from an attack, and to determine how critical the asset is based on its interdependencies with other transportation systems or facilities. Although these consequence estimates

³² DHS determined that the Tier 1 list criteria and all numbers related to the Tier list is "For Official Use Only." As a result, the related data are not contained in this report.

are a key component of an asset-specific risk assessment, not all critical highway assets have been subject to an SAV assessment to allow for consequence data to be evaluated nationwide to help establish protection priorities. Similarly, USCG also calculates consequence scores for all maritime critical infrastructure as a key component of its MSRAM analysis; however, not all of the nation's critical bridges and tunnels have a maritime nexus for which USCG analysis applies.

Federal Risk Assessment Activities Have Been Hampered by Limited Coordination

While federal entities are conducting a number of individual efforts to assess highway infrastructure risks, they have not systematically coordinated these efforts or shared the results. Federal entities have collectively conducted asset-level vulnerability assessments on a substantial percentage of highway infrastructure assets identified on the 2007 Tier 2 list. However, limited mechanisms exist to share the assessment results among the various federal partners to inform their own assessment efforts. For example, HMC reported that it is generally unfamiliar with the assessment processes, mechanisms, and results of the other DHS entities, particularly IP. Lacking adequate coordination mechanisms, the potential for duplication and inadequate leveraging of federal resources exists. For example, multiple vulnerability assessments were conducted by federal agencies for numerous assets that were on the fiscal year 2007 Tier 2 list. Specifically, IP and USCG conducted assessments on a number of the same assets identified as critical.³³ 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 amongst these entities.

As the SSA for highway infrastructure security, TSA is responsible for facilitating and coordinating risk assessment activities and protection efforts for these assets. As further specified in the NIPP, the SSA is responsible for the overall coordination and facilitation of comprehensive risk assessment programs for the sector, which include gathering all available threat, vulnerability, and consequence information from sector partners for use in national risk management efforts. Our previous work has also indicated that a key component for successful collaboration between federal agencies includes the effective leveraging of available

³³ According to USCG officials, risk assessments conducted by IP on the same infrastructure assets may be valuable to validate and inform its own MSRAM analysis.

resources.³⁴ While TSA is compiling limited vulnerability assessment information through its CSR program, no policies or mechanisms currently exist to coordinate this effort with those of other federal partners.³⁵ Considering that IP and USCG are conducting nearly all of the federal asset-specific vulnerability assessments completed to date, TSA is missing an opportunity to fully inform its vulnerability analysis for the highway infrastructure sector and validate the findings obtained from its CSRs.

While some efforts have been initiated by DHS entities to improve the coordination of highway infrastructure assessment activities, such actions have been limited. According to USCG officials, MSRAM analysis routinely includes the review of completed IP assessments of port-related infrastructure, including bridges and tunnels; however, coordination among the other two agencies is less mature. For example, HMC officials were generally unfamiliar with the scope of IP's SAV assessments and were unaware how these activities may be leveraged to achieve mutual goals. According to TSA officials, they had begun to receive notifications of IP assessments in July 2008; however, in September 2008, they stated that they generally do not review these assessments or incorporate the results.³⁶ HMC officials also stated that they have not reached out to obtain MSRAM data because they believe that port areas are well managed by USCG. Similarly, IP officials stated that they had not requested or reviewed the results of TSA's highway infrastructure CSRs. According to IP officials, a Protective Measures Section was created in fiscal year 2008 to consolidate and track IP assessments, as part of the Vulnerability Assessment Project. This project, as described in the IP Strategic Plan: FY 2008-2013, was originally intended to also provide a mechanism to track and analyze the vulnerability assessments conducted by other Federal, State, local, and private sector partners in order to enhance coordination and collaboration with stakeholders, eliminate duplication of effort, and enable assessment prioritization. However, OIP officials stated that, due to

³⁴ See [GAO-06-15](#).

³⁵ According to FHWA officials, they assisted in arranging and participated in several of the CSRs performed by TSA.

³⁶ According to DHS officials, the SSA Auto Notification System, provided through the Linking Encryption Network System (LENS), has resolved the issue of IP notifying to SSAs when they scheduled vulnerability assessments. The Auto Notification System sends an email to the SSA when an assessment has been scheduled, including the type of vulnerability assessment, a description of the assessment, trip dates, and further contact information are listed in the email.

a lack of funding, the scope of this effort was limited only to IP's own vulnerability assessments.³⁷

Another area where additional collaboration between federal partners may be improved involves the potential streamlining, or standardization, of existing assessment tools and methodologies. As outlined in the NIPP, vulnerability assessments need to be comparable to support national-level and cross-sector analysis. Further, HSPD-7 requires DHS to establish uniform policies, approaches, guidelines, and methodologies for integrating Federal infrastructure protection and risk management activities within and across sectors. However, a number of varied risk assessment tools and methodologies exist both within and across sectors that differ in terms of assumptions, comprehensiveness, and objectivity. Efforts to combine or streamline some of these tools and methodologies may assist to enhance the comparability and usefulness of the various risk assessments. For example, IP's Strategic Plan: FY 2008-2013, identifies opportunities for the development of a scalable methodology, in collaboration with other SSAs, to standardize current approaches for identifying vulnerabilities and promote better coordination and collaboration. USCG officials also cited the need for a comprehensive risk analysis model so that all sectors could utilize a common tool. According to the Highway Modal Annex to the TSSP, issued in May 2007, TSA was working with DOT agencies, including the Federal Motor Carrier Safety Administration (FMCSA) and FHWA, to combine their respective risk assessment and risk mitigation tools into a single product that will reduce redundancy, increase efficiencies, and minimize impact on private stakeholders. However, in October 2008, FHWA officials stated that this effort had not occurred.³⁸ The Modal Annex does not identify any additional plans for TSA to combine or incorporate any other key risk assessment tools, including USCG's MSRAM tool, IP's risk assessment and mitigation tools, or AASHTO's risk methodology. While the development of a single risk assessment tool that meets the individual needs of the distinct federal entities involved in highway infrastructure security may not be a realistic alternative, opportunities remain for DHS to identify

³⁷ According to DHS, IP's Protective Measures Section is to collect and analyze information to evaluate the effectiveness of assessments, protective measures implemented, and grant funding provided to high-priority CIKR.

³⁸ According to FHWA officials, representatives from TSA and FHWA met in December, 2008 to initiate planning efforts to combine risk assessment tools, where they deemed applicable.

where specific assessment tools and methodologies can be used most effectively to enhance assessments and better leverage future resources.

Effective coordination of federal vulnerability assessments and sharing of assessment results is more important given the number of highway infrastructure assets. Lacking adequate coordination with federal partners, TSA will be unable to determine the extent to which specific critical assets have been assessed and if potential adjustments in its own CSR methodology may be necessary to adequately target remaining critical infrastructure assets. Given the resource limitations and competing priorities of TSA and IP discussed previously, it is increasingly important for federal entities to coordinate their risk assessment activities and to share all available risk information to avoid duplication, better focus future assessments, and more effectively leverage resources.

DHS's Strategy to Secure Highway Infrastructure Was Not Fully Informed by Available Risk Information, and Should be Strengthened

While DHS has developed a strategy—the Highway Modal Annex—to secure the nation's highway infrastructure, it is not based on completed risk assessments to help ensure that federal programs and resources are focused on the areas of greatest need. Moreover, the Annex can be strengthened to better address the requirements of Executive Order 13416 on Strengthening Surface Transportation, and more fully incorporate characteristics of an effective national strategy. In addition, we identified areas where the Highway Modal Annex can be strengthened to enhance its value to highway security stakeholders by providing greater clarity of roles and focusing resources to protect highway infrastructure. TSA plans to revise the strategy in the near future, as required by the Annex and in accordance with TSA guidance, and officials stated that they would consider enhancing the Annex to address these areas at that time.

DHS's Highway Modal Annex Does Not Fully Incorporate Risk Assessment Results

In May 2007, TSA published the Highway Modal Annex which documents DHS's strategy for securing the nation's highway infrastructure;³⁹ however, while both the NIPP and the TSSP outline a framework whereby infrastructure protection efforts are to be guided by risk assessments of critical assets, the TSSP Highway Modal Annex is not fully informed by available vulnerability and consequence information. The Annex describes key TSA and FHWA programs related to highway infrastructure security efforts, as well as how transportation sector goals and objectives are to be

³⁹ Development and implementation of the Highway Modal Annex was conducted by HMC.

achieved to protect the highway transportation system. However, while nearly all of TSA's and IP's completed vulnerability assessments were conducted prior to the issuance of the Highway Modal Annex, their results were not used to develop the Annex. Both the NIPP and TSSP sets forth a comprehensive risk management framework which includes a process of considering threat, vulnerability and consequence assessments together to determine the likelihood of a terrorist attack and the severity of its impact. In addition, the TSA guidance used to assist each mode in drafting the Annex identifies that the Annex should emphasize how each mode will use risk informed decision-making to determine specific actions required to achieve the transportation sector goals and objectives. According to HMC officials, the Highway Modal Annex was developed in conjunction with the Highway GCC and SCC using available threat information, professional judgment, and information about past terrorist incidents. However, HMC officials stated that they did not review available IP and USCG vulnerability and consequence assessments of highway infrastructure—which represents the vast majority of asset-specific information. According to these officials, the initial development of the Highway Modal Annex was limited by time, which impacted HMC's ability to consider more comprehensive risk assessment information collected and incorporate stakeholder input.⁴⁰ However, officials stated that they anticipate that future revisions to the TSSP Highway Modal Annex will consider more risk assessment information and stakeholder input. In addition, HMC officials said that they are working on developing a separate national bridge strategy to supplement the Annex, but officials did not have a time frame for its completion.

According to TSA guidance used to develop the Highway Modal Annex, the Highway GCC and SCC are to review the Annex annually and make periodic interim updates as required, which provide TSA with an opportunity to consider the results of risk assessments to inform its strategy moving forward. The Highway GCC and SCC are instructed to conduct a complete revision of TSA's Highway Modal Annex every three years, and as necessary in the interim. HMC is beginning the revision process and updating the TSSP Highway Modal Annex in 2008 to allow time for the revised strategy to be reviewed by government and sector stakeholders. However, HMC officials stated that they did not know when the revision would be issued. Without considering the results of available

⁴⁰ Executive Order 13416 mandated that modal annexes were to be completed within 90 days after the comprehensive TSSP was completed.

risk assessments, TSA is limited in its ability to assist highway infrastructure operators in prioritizing investments based on risk, and target resources towards security measures that will have the greatest impact.

DHS's Highway Modal Annex Does Not Fully Address Areas Outlined in Executive Order

In reviewing the Highway Modal Annex, we identified areas in which the Annex does not fully address areas outlined in Executive Order 13416, Strengthening Surface Transportation Security, which was issued in December 2006 to address surface transportation security challenges consistent with the NIPP risk management framework. Executive Order 13416 requires that the Secretary of Homeland Security assess the security of each surface transportation mode and evaluate the effectiveness and efficiency of current surface transportation security initiatives. In addition, the Executive Order required the Secretary to develop modal annexes that include, at a minimum:

- an identification of existing security guidelines and requirements and any security gaps;
- a description of how the TSSP will be implemented for each mode, and the respective roles, responsibilities, and authorities of Federal, State, local, and tribal governments and the private sector;
- schedules and protocols for annual reviews of the effectiveness of surface transportation security-related information sharing mechanisms; and
- a process for assessing compliance with any security guidelines and requirements issued by the Secretary for surface transportation, and the need for revisions of such guidelines and requirements to ensure their continuing effectiveness.

Although Executive Order 13416 requires the identification of existing security guidelines and security requirements for each surface transportation mode, the Annex does not reference existing guidance developed by other federal and state highway infrastructure stakeholders including IP, FHWA, or AASHTO guidance on protective measures for highway infrastructure.⁴¹ TSA acknowledged that this information is missing from the Annex. Without including such information in TSA's national strategy for highway security, the agency is missing opportunities

⁴¹ TSA officials stated they are planning to issue best security practices for the entire highway mode on major topics including access control and vulnerability assessments to highway infrastructure stakeholders. HMC refers to this guidance as the U.S. (Universal Security) Template, but does not have a time frame for issuing this product.

to identify and leverage available guidance resources for securing highway infrastructure.

In addition, as called for in Executive Order 13416, the Annex does identify a number of existing security gaps related to highway infrastructure, and recognizes that addressing potential threats to the highway system is particularly challenging because of the openness of the system. However, while the Annex identifies that the conveyance of hazardous materials poses the greatest threat to highway infrastructure—and is where HMC has focused its efforts—the Annex provides little details about the different types of threats to highway infrastructure and their relative likelihood. For example, the Annex does not describe how terrorists might use explosives against highway infrastructure. According to the Annex, some bridges and tunnels are especially vulnerable because their structural components are in some cases easily accessible and because the assets themselves are located in remote areas.

Furthermore, Executive Order 13416 requires DHS to describe how the TSSP will be implemented within the specific transportation mode, yet we identified areas where the Annex could improve its description of how the TSSP would be implemented. For example, although not specifically required, the Annex lacks milestones. Specifically, the Annex does not indicate timeframes or milestones for its overall implementation or for accomplishing specific actions or initiatives for which entities can be held responsible. In addition, the Annex's priorities, goals and supporting objectives and activities are not ranked by their importance.

Executive Order 13416 also calls for Modal Annexes to include a description of the roles and responsibilities of key stakeholders, which the Highway Modal Annex only partially addresses because the Annex does not clearly define the authorities of federal, state, local, and tribal governments and the private sector to secure highway infrastructure. For example, the Annex does not identify that TSA has the authority to issue and enforce security related regulations and requirements it deems necessary to protect transportation assets. In addition, the Highway Modal Annex discusses the Highway GCC and Highway SCC roles and responsibilities related to highway and motor carrier security strategies and activities, as well as policies, guidelines and standards and developing program metrics and performance criteria for the mode. It also describes several TSA and FHWA highway related risk assessment programs involving collaboration with stakeholders. However, the strategy does not identify the specific roles of federal and non federal stakeholders such as HMC, IP, FEMA, CBP, FHWA, or AASHTO in the protection of critical

highway infrastructure or key assets. HMC officials attributed these omissions to the short turn around time required to develop the Annex. In addition, HMC officials stated that the Annex was vetted by a variety of stakeholders including IP, and no one raised concerns over the absence of a description of the roles of these federal and non federal entities and their programs. HMC officials stated that they were willing to consider including these entities in future revisions of the Annex. Moreover, the Annex does not identify lead, support, and partner roles related to highway infrastructure security. For example, CBP is responsible for prohibiting the entry into the United States of people or goods that pose a security threat; as well as the protection of the infrastructure within the footprint of the ports of entry, while TSA is responsible for the security of all modes of transportation, including any associated infrastructure.⁴² An overlap in responsibility exists when the people and goods crossing the border intend to harm infrastructure, e.g. a truck crossing a border bridge with the intention of exploding the bridge. Our prior work has highlighted the importance of addressing which organizations will implement a national strategy, their roles and responsibilities, and mechanisms for collaborating their efforts.⁴³

DHS's Highway Modal Annex Should Be Enhanced by Incorporating Characteristics of an Effective National Strategy

We assessed the Highway Modal Annex using desirable characteristics developed by our prior work on national strategies, and found several areas where future versions of the Annex can be enhanced.⁴⁴ Our prior work has shown that national strategies can be more useful if they contain characteristics such as a description of the purpose, scope, and methodology of the strategy; goals, objectives, activities, and performance measures; a definition of the roles and responsibilities and mechanisms for collaborating; the sources and types of resources and investments associated with a strategy; and a description of how a national strategy will be integrated with other national strategies and how it will be implemented. We believe that these characteristics can assist DHS in

⁴² CBP is not responsible for the bridges or tunnels that may lead to and/or away from the port of entry as they are not owned nor leased by CBP and are not a part of the footprint of the port of entry. Ports of entry are government-designated locations where CBP inspects persons and goods to determine whether they may be lawfully admitted into the country. A land port of entry may have more than one border crossing point where CBP inspects travelers for admissibility into the United States.

⁴³ [GAO-06-15](#).

⁴⁴ [GAO-04-408T](#).

strengthening and implementing the Highway Modal Annex going forward, as well as enhance its usefulness in resource and policy decisions and to better assure accountability.

Purpose, Scope, and Methodology

This characteristic addresses the purpose for developing the strategy, the scope of its coverage, and the process by which it was developed. In addition to describing what it is meant to do and the major functions, mission areas, or activities it covers, a national strategy would ideally address the methodology used to develop it. For example, a strategy might discuss the principles or theories that guided its development, what organizations or offices drafted the document, whether it was the result of a working group, or which parties were consulted in its development. The purpose and scope of the strategy are generally described in the Annex. For example, the Annex provides a description of the nation's highway transportation system and how transportation sector goals and objectives will be achieved to protect the highway transportation system. However, the Annex does not explain the methodology used in its development. For example, while the Highway Modal Annex references the NIPP and TSSP as providing the principles or theories that guided its development, the Annex does not describe the process and information that was used to develop it. HMC officials attributed this omission to the TSA guidance used to develop the Highway Modal Annex not requiring the process and information that was used to develop it be documented. HMC officials stated that stakeholders used their collective professional judgment to develop the Annex.

Goals, Objectives, Activities, and Performance Measures

This characteristic addresses what the national strategy strives to achieve and the steps needed to garner those results, as well as the priorities, milestones, and performance measures that will be used to gauge results. At the highest level, this could be a description of an ideal "end-state" of the strategy, followed by a logical hierarchy of major goals, subordinate objectives, and specific activities to achieve results. Our prior work has shown that long-term action-oriented goals and a time line with milestones are necessary to track an organization's progress toward its goals.⁴⁵ Ideally, a national strategy would set clear desired results and priorities, specific milestones, and outcome-related performance measures while giving

⁴⁵ GAO, Highlights of a GAO Forum: Mergers and Transformation: Lessons Learned for a Department of Homeland Security and Other Federal Agencies, [GAO-03-293SP](#) (Washington, D.C.: November 2002).

implementing parties flexibility to pursue and achieve those results within a reasonable timeframe.

While the Highway Modal Annex identifies individual, high-level goals, subordinate objectives, and specific activities to achieve results which are aligned with the specific goals and objectives identified in the TSSP, it does not describe key related activities. The Annex identifies three major goals—prevent and deter acts of terrorism using or against the transportation system, enhance resilience of the transportation system, and improve the cost-effective use of resources for transportation security. The three goals are underpinned by objectives, such as an objective supporting the goal of implementing flexible, layered, and effective security programs using risk management principles. The objectives in turn, have accompanying activities. For example, one of the supporting activities for the goal to prevent and deter acts of terrorism using or against the transportation system is HMC's CSR program. However, the Annex focuses on HMC and FHWA activities, but does not describe several key related federal and non federal activities. For example, the Highway Modal Annex does not describe the relationship of IPs Vulnerability Assessment program, USCG's risk assessment activities related to highway infrastructure, S&T Directorate's related research and development projects, AASHTO's security design standard development efforts, or CBP's activities related to international border crossings as they relate to supporting the Annex's goals and objectives.

In addition, one of the Annex's objectives is to enhance information and intelligence sharing among transportation security partners. Accordingly, the strategy identifies the Highway Information Sharing Analysis Center (ISAC) and the Homeland Security Information Network (HSIN) as two mechanisms to share information with the highway infrastructure stakeholders. However, the Annex does not discuss how HSIN complements or is different from other information sharing tools, such as DHS's Lessons Learned Information System (LLIS), as it concerns highway infrastructure. The Annex also does not discuss how HSIN is related to state efforts for sharing information. For example, during our review, one of the states we visited was developing a web site to share information for transportation security stakeholders which would potentially duplicate or overlap with information available through HSIN or LLIS.

Furthermore, TSA, in conjunction with the Highway GCC and the Highway SCC, has not developed a baseline set of performance goals and measures or established a time frame upon which to assess and improve preparedness of highway infrastructure to an attack that are linked to the

Annex's goals, objectives, and activities for securing highway infrastructure. The NIPP requires DHS to work with its security partners to develop sector-specific metrics. In addition, the Government Performance and Results Act (GPRA) as well as Standards for Internal Control in the Federal Government,⁴⁶ require that agencies use performance measurement to reinforce the connection between their long-term strategic goals and the day-to-day activities of their managers and staff. In addition, the Office of Management and Budget requires all programs to have at least one cost efficiency measure as part of their mix of performance measures. With respect to highway infrastructure security, performance measures would gauge to what extent federal efforts and highway infrastructure operators are achieving the Annex's goals and objectives. HMC officials stated that although they recognize the importance of measuring the effectiveness of security efforts, they have not developed performance measures for highway infrastructure. HMC officials attributed this omission to the TSA guidance used to develop the Highway Modal Annex not requiring performance measures. Without performance measures and an evaluation of the effectiveness of the Annex's goals and objectives, TSA will lack meaningful information from which to determine whether the strategy is achieving its intended results and to target any needed improvements.

Organizational Roles, Responsibilities, and Collaboration

This characteristic addresses which organizations will implement the strategy, their roles and responsibilities, and mechanisms for coordinating their efforts. It helps answer the fundamental question about who is in charge, not only during times of crisis, but also during all phases of homeland security and combating terrorism efforts: prevention, vulnerability reduction, and response and recovery. This characteristic entails identifying the specific federal departments, agencies, or offices involved and, where appropriate, the different sectors, such as state, local, private, or international sectors. In our past work, we reported that a successful strategy clarifies implementing organizations' relationships in terms of leading, supporting, and partnering. In addition, a strategy could describe the organizations that will provide the overall framework for accountability and oversight. Furthermore, a strategy might identify specific processes for collaboration between sectors and organizations—and address how any conflicts would be resolved. For example, our previous work on effective interagency collaboration has also

⁴⁶ Pub. L. No. 103-62, 107 Stat. 285 (1993); and [GAO/AIMD-00-21.3.1](#).

demonstrated that a strategy provide for some mechanism to ensure that the parties are prepared to fulfill their assigned responsibilities.⁴⁷

The Annex provides limited information related to collaboration between highway infrastructure stakeholders. In addition, the 9/11 Commission Act requires DHS and DOT to execute and develop an annex to the memorandum of understanding (MOU) between the two agencies, which was signed in September 2004, that addresses motor carrier security.⁴⁸ The annex must delineate specific roles, responsibilities, and resources needed to address motor carrier transportation security matters and the processes the Departments will follow to promote communications, efficiency, and ensure non duplication of effort. HMC officials stated that they plan on developing a similar annex to the MOU for highway infrastructure, but they do not have a timetable for doing so. Our prior work has shown that collaboration between federal stakeholders can be improved by clearly identifying organizational roles, responsibilities and specific processes for collaboration between sectors—and how any conflicts would be resolved. HMC officials stated that such an annex would serve to lay the groundwork and provide the proper protocols for sharing of data and personnel, and acknowledge leadership roles and responsibilities to strengthen highway infrastructure security.

The 9/11 Commission Act also requires that DHS, to the greatest extent practicable, provide public and private stakeholders with transportation security information in an unclassified format.⁴⁹ The Highway Modal Annex provides limited details on how (process, policy, mechanism) it will collaborate or what is needed to enhance information and intelligence sharing. For example, the Annex does not describe HITRAC's role related to information sharing. HITRAC is a joint organization between IP and the Critical Infrastructure Threat Analysis Division within I&A that is to integrate, analyze, and share information regarding threats and risks to U.S. critical infrastructure for DHS, other federal departments and stakeholders, the intelligence community, state and local governments and law enforcement stakeholders, and the private sector. HMC officials attributed this omission to the TSA guidance used to develop the Highway Modal Annex not requiring a description of how it is to collaborate or what

⁴⁷ See [GAO-04-408T](#).

⁴⁸ Pub. L. No. 110-53, § 1541, 121 Stat. 266, 469 (2007).

⁴⁹ *Id.* at § 1203(a)(9), 121 Stat. at 386 (codified at 49 U.S.C. § 114(u)(9)).

is needed to enhance information and intelligence sharing. The Act also required DHS to establish a plan to share transportation information relating to the risks to transportation modes, including the highway mode that was due in early 2008; however the plan has not yet been completed.⁵⁰ TSA officials said that DHS was developing the information sharing plan, but they did not know when the plan would be issued. Development of a plan could improve information sharing by clarifying roles and responsibilities and clearly articulating actions to address any remaining challenges, including consideration of appropriate incentives for nonfederal entities to increase information sharing with the federal government, increase sector participation, and perform other specific tasks to protect critical highway infrastructure.

Resources and Investments

This characteristic addresses what the strategy will cost, the sources and types of resources and investments associated with the strategy, and where those resources and investments should be targeted. Ideally, a strategy would also identify criteria and appropriate mechanisms to allocate and take in resources—such as grants, in-kind services, loans, and user fees—based on identified needs. Alternatively, as our prior work has shown, the strategy might identify appropriate “tools of government,” such as regulations, tax incentives, and standards, to mandate or stimulate nonfederal organizations to use their unique resources.⁵¹

The Highway Modal Annex does not describe any incentives that could be used to encourage owners to conduct voluntary risk assessments, such as grants or training that could be used to determine the best courses of action to reduce potential consequences, threats, or vulnerabilities, as required by the NIPP. These incentives are important because asset owners are not currently regulated by TSA. According to HMC officials, the guidance provided by TSA to HMC used to develop the Highway Modal Annex did not require a description of possible incentives. In addition, HMC officials said that they are working on developing a separate national bridge strategy to supplement the Annex. According to HMC officials the national bridge strategy is to assist the stakeholder community in assessing both the criticality and the security vulnerabilities of its assets; identify the most appropriate and cost-effective mitigation tools; and serve as a mechanism for the identification of sources of funding that are exclusively dedicated to security needs and do not require diversion of

⁵⁰ *Id.* at § 1203(a)(2), 121 Stat. at 384 (codified at 49 U.S.C. § 114(u)(2)).

⁵¹ [GAO-04-408T](#).

funding that is otherwise reserved for safety or structural enhancement or refurbishment. However, this effort is not completed and HMC does not have a time frame for its implementation.

In addition, the Annex identifies that measures to secure assets of the Highway Transportation System must be implemented in a way that balances cost, efficiency, and preservation of the nation's commerce; however, it provides relatively few details on the types and levels of resources associated with implementation of security measures or where to target resources for securing highway infrastructure. Highway infrastructure operators have received some federal funding for implementing security upgrades since September 11th, 2001, but available funding has been limited due to competing priorities, such as dams and nuclear facilities. Targeting investments is especially important given that the current economic environment makes this a difficult time for private industry or state and local governments to make security investments.

Integration and Implementation

This characteristic addresses both how a national strategy relates to other strategies' goals, objectives, and activities, and to subordinate levels of government and their plans to implement the strategy. For example, a national strategy could discuss how its scope complements, expands upon, or overlaps with other national strategies. Similarly, related strategies could highlight their common or shared goals, subordinate objectives, and activities. In addition, a national strategy could address its relationship with relevant documents from implementing organizations, such as the strategic plans, annual performance plans, or annual performance reports. A strategy might also discuss, as appropriate, various strategies and plans produced by the state, local, private, or international stakeholders.

The Highway Modal Annex contains certain elements of this characteristic, but it lacks a description of how it relates to other strategies. For example, the Annex references FHWA's Multiyear Plan for Bridge and Tunnel Security Research, Development, and Deployment, which highlights efforts to secure the nation's highway infrastructure. However, the Highway Modal Annex does not define its relationship with other related strategies or federal actions, or address its relationship with other plans by federal, state, local, and international implementing parties. Specifically, although TSA is engaged in three strategic planning initiatives that have similar goals but slightly different requirements, the Annex does not discuss its relationship to these strategies. First, the Intelligence Reform and Terrorism Prevention Act of 2005 requires a strategy for transportation security—the National Strategy for Transportation Security

(NSTS)— containing the identification and evaluation of transportation assets and appropriate mitigation approaches. Second, the NIPP and HSPD-7 require each sector to prepare a sector specific plan, in collaboration with its security partners across government and private industry. Third, Executive Order 13416 contains requirements for developing modal annexes to the TSSP for surface modes of transportation. However, the Annex does not discuss how its scope complements, expands upon, or overlaps with these strategic plans and guidance. In addition, the Annex does not discuss how the programs in IP's strategic plan complement or overlap with the Highway Modal Annex. Without such information in TSA's national strategy for highway security, the agency is missing opportunities to build on organizational roles and responsibilities and further clarify relationships, which could improve the strategy's implementation.

Government and Industry Stakeholders Have Efforts Underway to Enhance the Security of Highway Infrastructure, but TSA Lacks a Mechanism to Monitor Implementation of Voluntary Security Measures

Government and industry highway sector stakeholders have taken actions to mitigate the risks to highway infrastructure through a combination of efforts, including developing publications and conducting seminars, sponsoring research and development activities, and implementing specific infrastructure protection measures. However, because HMC does not routinely conduct asset-specific assessments of highway infrastructure, TSA does not have a mechanism to monitor the implementation of both government and industry voluntary security enhancements put in place to address identified asset vulnerabilities and help protect the nation's critical highway infrastructure. TSA is tasked with assessing and evaluating the effectiveness and efficiency of current federal government surface transportation security initiatives. According to TSA officials, such a monitoring mechanism for voluntary efforts is not necessary because TSA obtains the information that it needs to monitor highway infrastructure security efforts through HMC's CSR efforts. However, the CSRs are at a high level and do not provide a means to assess the protective security measures implemented for specific assets. Lacking a mechanism to monitor the implementation of protective security measures, TSA cannot evaluate the effectiveness of existing programs and assessing the overall security preparedness of the nation's critical highway infrastructure.

The Federal Government, States, and Other Highway Stakeholders Have Voluntary Efforts Underway to Enhance the Security of Highway Infrastructure

Highway sector stakeholders have taken a variety of voluntary actions intended to enhance the security of highway infrastructure. Key efforts include developing security publications, sponsoring infrastructure security workshops, conducting research and development activities, and implementing specific protective measures intended to deter an attack or reduce potential consequences, such as security patrols, electronic detection systems, and physical barriers. Overall, these programs and activities are intended to provide asset owners and operators with tools and guidance for assessing highway infrastructure security risks, highlight effective practices in security planning and vulnerability reduction, and share technical expertise and information for enhancing asset security. See table 2 for a summary of key highway infrastructure security programs and activities.

Table 2: Summary of Key Programs and Activities to Enhance Security of Highway Infrastructure

Key Programs and Activities	Description	Responsible Organizations
Publications, Guidance, and Training		
Bridge and Tunnel Workshops	These workshops, introduced in fiscal year 2004, are intended to provide participants with information about identifying infrastructure risks and developing appropriate mitigation measures. As of January 2009, FHWA had conducted a series of workshops, targeted primarily to bridge and tunnel engineers and asset operators, in 28 locations.	FHWA
Publications	<p>Since 2002, AASHTO, through the Transportation Research Board (TRB), has sponsored or developed several key publications to help asset owners identify critical assets, perform risk assessments, and evaluate potential countermeasures. At the request of AASHTO and FHWA, in 2003, a Blue Ribbon Panel was convened to prepare recommendations for bridge and tunnel security.</p> <p>FHWA has also issued security-related publications, such as the Multi-Year Plan for Bridge and Tunnel Security Research Development and Deployment, and an article entitled Risk Management for Terrorist Threats to Bridges and Tunnels.</p> <p>IP has developed several reports identifying general threats and common vulnerabilities for highway infrastructure assets.</p>	TRB, AASHTO, FHWA, IP

Key Programs and Activities	Description	Responsible Organizations
Regional Conferences	In cooperation with AASHTO, TSA and FHWA co-sponsored a series of regional infrastructure protection conferences for state DOT officials. These conferences provided an opportunity for participants to exchange information concerning effective security practices and communicate security concerns and implementation challenges.	TSA, FHWA, AASHTO
Research and Development		
Transportation Sector Research & Development Working Group	With broad-based federal and state representation, this group serves to identify potential research areas for the highway sector.	TSA, IP, FHWA, State DOTs
DHS Science & Technology (S&T)	S&T is responsible for executing multiple highway research projects based on identified needs and national risk priorities. Several bridge and tunnel projects have been initiated in recent years (see appendix IV for additional project details).	DHS S&T
Cooperative Research Programs	The TRB, through its Cooperative Research Programs, produced a number of reports each year addressing highway research issues, such as Recommendations for Bridge and Tunnel Security, and a guide to making transportation tunnels safe and secure.	TRB, FHWA, AASHTO
Transportation Pooled Fund Study (TPFS)	This program consists of pooled funds provided by individual states and other agencies, including TSA, to conduct research or provide training or education materials desired by the contributors. FHWA is currently managing several projects, including the development of training materials in the areas of security and emergency management, and development of blast mitigation measures for critical bridges.	FHWA
Protective Security Measures		
Owner/Operator Funded Security Measures	States and other highway infrastructure asset owners/operators have implemented a variety of protective security measures, including security patrols, cameras and other detection equipment, physical barriers, and security awareness training, among others. According to state officials, funding represents the principal constraint to implementation of security measures.	Highway Asset Owners/Operators

Key Programs and Activities	Description	Responsible Organizations
Grant Programs	<p>FEMA manages DHS grant programs and has allocated funds to state and local stakeholders for highway security enhancements through two primary programs—the Homeland Security Grant Program and the Infrastructure Protection Program. Since 2004, approximately \$34 million has been allocated to projects related, in part, to highway infrastructure security.</p> <p>The Trucking Security Program (TSP), within the Infrastructure Protection Program, provides funds to assist professionals and operating entities in the highway sector to develop awareness of potential highway-related security concerns. The program also includes a 24-hour call center for the anti-terrorism and security awareness program, and the Highway Information Sharing and Analysis Center (ISAC) for investigation of terrorist threats. While FEMA has the lead for the administrative mechanisms needed to manage the TSP, TSA provides subject matter expertise and oversight. A grantee is responsible for the day to day operations of these efforts.</p> <p>IP guides the allocation of BZPP grant funds, part of the Infrastructure Protection Program, administered by FEMA, and shares in overall programmatic oversight and final decision-making authority with FEMA.</p>	FEMA, TSA, IP
Protective Security Advisor (PSA) Program	<p>These individuals serve as liaisons between Federal stakeholders, state and local governments, and the private sector. Their principal roles and responsibilities include identifying, assessing, monitoring, and mitigating risk to high-risk critical infrastructure and key resources at the local level. PSAs are knowledgeable of all high-priority critical infrastructure and key resources across the various sectors, within their area of responsibility.</p>	IP

Source: GAO analysis of highway infrastructure security related programs and activities.

Publications, Guidance, and Training

Highway infrastructure stakeholders have developed a number of products and programs intended to facilitate the identification of critical assets and provide guidance for conducting security planning. Many of these products and programs are conducted as joint efforts between the State highway agencies, represented by AASHTO and federal partners, including TSA, FHWA, and the Transportation Research Board (TRB). Since 2002, AASHTO, through TRB’s Cooperative Research Programs, sponsored or developed several key publications that serve to assist states in identifying critical assets, perform risk assessments, and evaluate options for reducing asset vulnerabilities, including providing a characterization of potential costs and challenges associated with infrastructure security enhancements.⁵² According to AASHTO, all state

⁵² *A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection*, Science Applications International Corporation, May 2002; *National Needs Assessment for Ensuring Transportation Infrastructure Security*, Parsons Brinckerhoff & Science Applications International Corporation, October 2002.; *Protecting America’s Roads, Bridges, and Tunnels: The Role of State DOTs in Homeland Security*, AASHTO, January 2005.

DOTs have access to, and a large majority (84 percent) are using, AASHTO guidance on vulnerability and criticality assessment, and risk management, to determine the extent and nature of vulnerabilities to their state's transportation systems. As discussed previously, IP has also developed and issued several reports to provide sector stakeholders guidance on security measures, and identifies general threats and common vulnerabilities for highway infrastructure assets.⁵³ In addition, IP provides stakeholders with guidance on security measures to implement based on homeland security advisory system threat levels. According to IP officials, these reports are made available to industry stakeholders via an internet portal.⁵⁴

TSA, FHWA, and AASHTO have also co-sponsored a series of regional conferences to facilitate the exchange of information about effective security practices and communicate stakeholder concerns and implementation challenges.⁵⁵ These conferences provide state transportation officials with a forum to share knowledge concerning infrastructure protection methods and help them identify potential training and guidance resources available. In a separate effort, FHWA also provided risk management training to bridge and tunnel engineers, asset operators, and first responders through a series of workshops. These workshops, introduced in 2003, are intended, in part, to provide highway infrastructure stakeholders a methodology for identifying vulnerabilities and developing appropriate and cost-effective risk mitigation plans. In addition, a security awareness training program is provided as part of the Trucking Security Program directed at highway sector professionals, which includes truck and motor coach drivers, highway engineers, and law

⁵³ Referred to as the "Collective Protection Papers," IP has produced a number of products to provide sector stakeholders guidance on security measures and specifically addresses the threats and vulnerabilities of highway infrastructure assets. These reports include: *Characteristics and Common Vulnerabilities-Infrastructure Category: Highway Bridges*; and *Potential Indicators of Terrorist Activity-Infrastructure Category: Highway Bridges*, among others.

⁵⁴ We did not assess the extent to which these products were being utilized by stakeholders when conducting vulnerability assessments.

⁵⁵ These conferences have been conducted in three locations. As of January 2009, TSA did not have any additional workshops scheduled.

enforcement, to identify and report suspicious activity on the nation's highway system.⁵⁶

Research and Development

A collection of research and development activities designed to secure highway infrastructure are currently being conducted by federal and state entities. As outlined in the Homeland Security Act of 2002, DHS is responsible for, among other things, working with federal laboratories and the private sector to develop innovative approaches to address homeland security challenges. Within the highway sector, these activities include research on the vulnerabilities of bridges and tunnels to various types of explosives and experimental methods to help protect these assets. At the federal level, research and development activities are coordinated through the DHS Transportation Sector Working Group. With fairly broad-based representation—including representatives from TSA, IP, S&T Directorate, FHWA, and state DOTs, among others—this group serves to identify potential research areas, which are then prioritized by IP and executed by DHS' S&T Directorate. According to S&T officials, highway infrastructure has been a focus of infrastructure security research efforts in recent years. Since 2005, bridges, in particular, have been prioritized to gain a better understanding of their potential vulnerabilities and identify better retrofit techniques. Some individual projects identified through this effort include the development of measures to reduce the vulnerability of flooding in underwater tunnels and potential attacks to bridge cables, as well as understanding failure mechanisms and mitigation against explosive attacks and other cross cutting research. See Appendix IV for a list of selected highway infrastructure research and development projects.

Other key research programs include the National Cooperative Highway Research Programs (NCHRP) administered by the Transportation Research Board TRB and FHWA's Transportation Pooled Fund Study program. Through the NCHRP Cooperative Research Programs, a number of research projects are conducted each year addressing highway-related

⁵⁶ The security awareness security program is funded through DHS' Trucking Security Program (TSP). For 2008, Congress appropriated \$16 million to administer the TSP (approximately \$77.8 million in total funds have been provided since fiscal year 2003). In September 2008, the DHS Inspector General identified several areas where the TSP program could be improved to enhance accountability and help ensure the viability of the program. Department of Homeland Security Inspector General, Effectiveness of the Federal Trucking Industry Security Grant Program, OIG-08-100 (Washington, D.C.: Sept. 26, 2008).

research issues proposed by AASHTO.⁵⁷ Although highway infrastructure security comprises just one component of the program's research portfolio, several security-related products have been developed in recent years. Some of these products include guidance on securing transportation tunnels and a tool to estimate the impact of disruption of key transportation choke points.⁵⁸ The Transportation Pooled Fund Study is a separate program, administered by FHWA, whereby states and other agencies contribute to a pooled fund to conduct research or provide training or education materials desired by the contributors. Some proposed products include the development of experimentally verified mitigation measures, clearly defined roles and responsibilities for State DOTs in infrastructure security, risk management training tailored to bridge and tunnel vulnerability assessments, and the development of blast mitigation measures for steel bridge towers and a bridge surveillance and security technology database, among others.

Protective Security Measures

While federal stakeholders play a role in facilitating risk-based infrastructure security efforts, the actual implementation of asset-specific protective security measures remains the responsibility of individual asset owners and operators, most commonly states or other public entities. Unlike some other transportation modes, such as commercial aviation, no federal laws explicitly require highway infrastructure owners to take security actions to safeguard their assets against a terrorist attack. The protection of highway infrastructure is being undertaken using a voluntary approach, although TSA retains the authority to issue and enforce security related regulations and requirements it deems necessary to protect transportation assets. According to HMC officials, TSA's decision to implement a voluntary approach to highway infrastructure security is based on available threat information, as well as information obtained during CSR activities, which indicates to them that states are generally aware of their security responsibilities and are implementing protective actions. In addition, HMC officials stated that a voluntary approach to security requires reduced federal resources and provides a greater amount

⁵⁷ The Transportation Research Board is one of six divisions of the National Research Council in the National Academies. The Board provides leadership through research and information exchange. The program is supported by state transportation departments, federal stakeholders including the component administrations of DOT, and other organizations and individuals interested in the development of transportation.

⁵⁸ According to FHWA, a new Cooperative Research Program study will soon be published by AASHTO entitled, "Costing Asset Protection: An All Hazards Guide for Transportation Agencies."

of buy-in and acceptance from asset owners than government regulations. Asset owners have implemented a range of voluntary protective security measures to help ensure public safety and protect their highway infrastructure assets. For example, asset owners commonly employ measures such as cameras or other surveillance equipment, and install fencing and other physical barriers to control access to vulnerable structures, among other protective measures. (See appendix III for additional examples of protective security measures for highway infrastructure assets). Specific mitigation measures typically fall into three broad categories:

- **Deterrence and Detection.** These mitigation measures secure access to restricted areas and reduce the likelihood of a potential attack. Common protective security measures include installing fencing, improving lighting, conducting security patrols and installing electronic detection systems.
- **Defense.** Defensive measures are intended to reduce the consequences of a successful attack. For example, installation of a physical barrier around vulnerable components or systems, such as a bridge pier, may reduce the impact of an explosive blast on the structure.
- **Design and Redesign.** These efforts are intended to harden planned or existing infrastructure assets against potential attacks by incorporating security considerations into engineering designs.

According to highway infrastructure operators, factors such as competing priorities and budgetary constraints greatly influence whether security measures are implemented. One principal factor impacting the implementation of security measures identified by some state officials we spoke to concerns the availability of revenue sources to fund security improvements for individual assets. For example, bridges and tunnels funded by user fees, such as tolls, could generate additional revenue for security enhancements. Alternately, mitigation measures financed with general federal and state transportation funds may be limited due to competing state priorities. However, the federal government has provided funds to state and local stakeholders to implement highway infrastructure improvements through a combination of several FEMA grant programs. Since 2004, FEMA has funded 60 highway-related security projects, totaling approximately \$34 million (see table 3). Some of these projects include funding for additional cameras and surveillance equipment, watercraft for investigation and response to threats, and interoperable communication equipment, among others.

Table 3: FEMA Grant Funding for Highway Infrastructure-Related Security Projects, 2004 to 2007

Grant Year	Number of Highway-Related Projects	FEMA Grant Funding for Highway-Related Projects ^a
2004	23	\$16,981,204
2005	23	5,703,092
2006	11	8,431,666
2007	3	2,844,538
Total	60	\$33,960,501

Source: GAO analysis of FEMA data.

^aAn initial list of potential highway-related projects was provided by FEMA using a keyword search of Biannual Strategy Implementation Reports. These reports—required by FEMA to be updated every six months as part of its grant monitoring process—are comprised of self-reported data submitted by grantees describing their use of allocated grant funds. To determine the total number of projects included in this analysis, we reviewed each of the project descriptions and omitted those that did not clearly have a component related to highway security. For example, a number of projects were specific to mass transit tunnels or railroad bridges and consequently, were not included. In addition, 22 of the projects that GAO identified above were targeted only in part to highway security, such as the purchase of patrol boats or interoperable communications equipment for first responders.

States have generally taken actions to help secure their highway infrastructure; however, wide variation exists regarding the implementation of specific protection efforts. According to TSA’s 2006 summary of its CSRs, all of the states polled have completed at least some security-related actions among the 11 functional areas assessed by TSA.⁵⁹ However, TSA reported that the level of implementation of security actions varied between states. For example, TSA reported that background checks of transportation workers conducted by state agencies ranged from a criminal history check driving records and citizenship checks down to reference checks for employment applications. According to TSA, the need for background checks varied from state to state, since the perceived threat and the level of risk tolerance also vary by state. In another example, most of the states responded that they conducted security planning at the state level; however, according to TSA, state governments vary considerably in the way the security plans are organized. For example, they reported that states assign different security functions to different agencies—particularly for transportation security

⁵⁹ TSA Transportation Sector Network Management Office - Highway and Motor Carrier Division, *Assessment of Highway Mode Security: Corporate Security Review Results*, May 2006. The 11 functional areas are: threat assessment, vulnerability assessment, security planning, credentialing, secure areas, critical infrastructure, physical security, cyber security, security training, communications and exercises.

functions. Each agency does some level of planning to ensure its ability to perform its functions. As a result, these preparations are documented in different places, including emergency response plans, traffic management plans, hazardous materials management plans, National Guard plans, homeland security advisory level preparedness plans, continuity of operations plans, and police patrol plans. Some of the plans are more complete than others, depending on the diligence of the agency. TSA reported that most of these states were able to produce a document that defined basic responses to different threat levels and defined who was in charge. Similar variation in state responses and the scope of individual efforts were also illustrated in several of the other security-related functional areas.

The variation in state security efforts identified by TSA is generally consistent with what we identified during interviews with officials and observations of select highway infrastructure in five states.⁶⁰ Although the specific protective security measures implemented at the 13 individual assets we visited were varied, we identified some common mitigation themes, such as investment in new security equipment, leveraging law enforcement resources, and identifying incident response roles, among others. Specific protective measures identified by asset owners with whom we spoke, include increased surveillance efforts—adding cameras and other detection equipment—as well as installation of fencing, physical barriers, and implementation of enhanced access controls. In addition, some state officials we interviewed stated that they restricted access to building designs and response plans, increased their patrol of critical structures, and implemented stand-off distances.

TSA Lacks a Mechanism to Monitor the Implementation of Protective Security Measures for Critical Infrastructure

Although government and industry stakeholders have taken actions to address the risks to highway infrastructure, TSA lacks a mechanism to determine the extent to which specific protective security measures have been implemented for critical assets. Such a mechanism is important to evaluate the security preparedness of nationally critical infrastructure assets and to help ensure that TSA's voluntary approach to highway infrastructure security remains adequate. For example, a monitoring mechanism would provide TSA with feedback regarding how its existing programs and security initiatives, in conjunction with highway

⁶⁰ To observe security measures undertaken by highway infrastructure operators, we selected a non-probability sample of 13 bridges and tunnels in 5 states to visit.

stakeholders, are translating into specific security actions by asset owners. TSA is tasked with assessing the security of each transportation mode and evaluating the effectiveness and efficiency of current federal government surface transportation security initiatives.⁶¹ In addition, Standards for Internal Control in the Federal Government generally calls for controls to be designed to ensure that an agency has relevant and reliable information about programs and that ongoing monitoring occurs.⁶² However, TSA has not documented how it will monitor the industry's progress in implementing voluntary highway infrastructure protective security measures for assets identified as nationally critical.

Although various federal entities have issued suggested security measures to asset owners, the extent that they have been implemented remains unclear. DHS risk assessment activities, including the CSR and SAV programs, identified highway infrastructure assets that would benefit from additional security measures and have suggested a number of voluntary protective actions to asset owners to address these enhancements. However, given the voluntary nature of these programs, TSA, IP, and USCG stated that they do not know the extent to which asset owners are implementing the protective security measures identified by completed risk assessments for critical infrastructure. In addition to competing resource priorities previously identified, IP officials stated that monitoring the implementation of voluntary protective security measures remains difficult due to limited resources. Specifically, they stated that IP does not have the resources needed to conduct follow-up assessments on all Tier 1 and Tier 2 assets across all critical infrastructure and key resources. They also noted that repeated visits may create a burden on private sector partners. In 2008, IP implemented the Enhanced Critical Infrastructure Protection initiative. This effort involves sending PSAs to all Tier 1 and 2 assets, including transportation infrastructure. According to DHS, while this is a voluntary, non-regulatory program, PSAs conduct initial and follow-up visits to CIKR and document the implementation of enhanced security and protective measures. According to HMC officials, the completion of a second round of state CSR visits will provide an opportunity to review whether asset owners are implementing previous CSR-related security considerations; however, the follow-up visits will be performed over a four year cycle and will not be conducted at the asset

⁶¹ Executive Order 13416, Strengthening Surface Transportation Security, December 5, 2006.

⁶² [GAO/AIMD-00-21.3.1](#).

level. While these efforts are a positive step, they do not provide the type of detailed information necessary to ensure that specific highway infrastructure assets, particularly those deemed nationally critical, are protected. According to TSA officials, the collection of more detailed data about protective measures is not currently feasible given available resources and other security priorities. However, HMC officials have stated that alternative cost-effective methods of collecting this information may be available, such as potentially leveraging the resources of state transportation inspectors during biannual bridge safety inspections. According to these officials, this program would provide a means to assess the protective security measures implemented for specific assets.

Lacking a mechanism to monitor what protective security measures are being implemented to protect the nation's critical highway infrastructure assets, TSA is unable to determine, with any degree of certainty, the level of overall security preparedness of these assets. In addition, without a process in place to better understand what security measures owners and operators are implementing, TSA is not effectively utilizing available information to help identify potential security gaps, establish protection priorities, and determine what, if any, additional measures may be needed to enhance highway infrastructure security.

Conclusions

Securing the nation's vast and diverse highway infrastructure is a daunting task. The nature, size, and complexity of this infrastructure highlights the need for federal and non-federal entities to work together to secure these assets and enhance security. While the cost of enhancing highway infrastructure security can be significant, the potential costs of a terrorist attack, in terms of both the loss of life and property and long-term economic impacts, would also be significant although difficult to predict and quantify. The importance of the nation's highway infrastructure and the limited resources available to protect it underscore the need for a risk management approach to prioritize security efforts so that a proper balance between costs and security can be achieved. By not fully evaluating the risks posed by terrorists to the nation's highway infrastructure through available assessments, TSA and its security partners are limited in their ability to focus resources on those highway infrastructure vulnerabilities that represent the most critical security needs. The large and diverse group of stakeholders involved in highway infrastructure security makes it difficult to achieve the needed cooperation and consensus to move forward with security efforts. As we have noted in past reports, coordination and consensus-building are critical to the successful implementation of security efforts. By

coordinating risk assessment activities and sharing the results of risk assessments, DHS could more effectively use scarce resources to target further assessment activities and mitigate identified risks.

By developing the Highway Modal Annex for highway infrastructure, TSA established strategic goals and objectives, a key first step in implementing a risk management approach. However, highway infrastructure stakeholders could benefit from a Highway Modal Annex that clearly describes their roles, responsibilities, relationships, and expectations for securing highway infrastructure and provides accountability for accomplishing its objectives. Moreover, performance measures developed in conjunction with the Highway GCC and SCC are important to assist TSA in evaluating the effectiveness of highway infrastructure programs, based on desired results that are defined by the Annex. Without performance measures, TSA may not have information with which to systematically assess these program's strengths, weaknesses, and performance. Additional guidance on where to target resources and investments would help implementing parties allocate resources and investments according to priorities and constraints, track costs and performance, and shift such investments and resources as appropriate.

We recognize that the Highway Modal Annex is not an endpoint for communicating and providing a framework for protecting highway infrastructure, but rather, a starting point. As with any planning effort, implementation is the key. The ultimate measure of this strategy's value will be the extent to which it proves useful as guidance for policy and decision-makers in allocating resources and balancing highway infrastructure security priorities with other important, non-highway infrastructure security objectives. It will be important over time to obtain and incorporate feedback from the stakeholder community as to how the strategy can better provide this guidance, and how Congress and the executive branch can identify and remedy impediments to implementation, such as legal, jurisdictional, or resource constraints. Finally, while the varied actions government and industry stakeholders have taken to address the risks to highway infrastructure are important initial efforts, without a mechanism to monitor what protective security measures are being taken to secure nationally critical infrastructure, TSA cannot fully determine the extent of security preparedness across the nation's highway infrastructure.

Recommendations for Executive Action

We are recommending that the Secretary of Homeland Security take the following three actions:

- To enhance collaboration among federal entities involved in securing highway infrastructure and better leverage federal resources, we recommend that the Secretary of Homeland Security establish a mechanism to systematically coordinate risk assessment activities and share the results of these activities among the federal partners.
- To help ensure that highway infrastructure stakeholders are provided with useful information to identify and prioritize potential infrastructure security measures, enhance future planning efforts, and determine the extent to which specific protective security measures have been implemented, we recommend that the Secretary of Homeland Security direct the Assistant Secretary for the Transportation Security Administration, in consultation with the Highway Government Coordinating Council and the Highway Sector Coordinating Council, to take the following actions:
 - (1) for the upcoming revision to the Highway Modal Annex:
 - in addition to the results of threat assessment information, incorporate the results of available vulnerability, and consequence assessment information into the strategy for securing highway infrastructure;
 - consistent with Executive Order 13416 and desirable characteristics of an effective national strategy, identify existing guidance developed by other federal and state highway infrastructure stakeholders; indicate timeframes or milestones for its overall implementation for which entities can be held responsible; more clearly define security-related roles and responsibilities for highway infrastructure security activities for itself and other federal stakeholders, state and local government, and the private sector; establish a timeframe for developing performance goals and measures for monitoring the implementation of the Annex's goals, objectives, and activities; and provide more guidance on resources, investments and risk management to help implementing parties allocate resources and investments according to priorities and constraints; and
 - (2) develop a cost-effective mechanism to monitor the implementation of voluntary protective security measures on highway infrastructure assets identified as nationally critical.

Agency Comments and Our Evaluation

We provided a draft of this report to DHS for review and comment. DHS provided written comments on January 21, 2009, which are presented in Appendix VI. In commenting on the draft report, DHS and TSA reported

that they concurred with all three of our recommendations and have started to develop plans to implement these recommendations.

With regard to our first recommendation that DHS establish a mechanism to systematically coordinate risk assessment activities and share the results of these activities among federal partners, DHS stated TSA will have the lead in developing a sector coordinated risk assessment. TSA stated that it recognizes that it is responsible for all transportation security matters, must fulfill its leadership role in the highway infrastructure arena, and is prepared to assume responsibility for all highway infrastructure security issues. TSA added that it will request of all DHS, DOT and State or local governmental bodies that TSA become the repository for all risk assessment models and data associated with this mode. Toward this goal, DHS stated that TSA has convened representatives of both DHS and DOT agencies to produce the “National Strategy for Highway Bridge Security,” which is currently under review by agencies and offices within both Departments. Once fully vetted, DHS believes that this document will provide for appropriate participation and coordination of efforts by all Federal agencies engaged in highway infrastructure security. We support TSA’s efforts to improve coordination and develop the National Strategy for Highway Bridge Security. The intent of our recommendation is to help DHS avoid potential duplication, better focus future assessment efforts, and leverage limited resources. Thus, if TSA’s efforts result in a mechanism that systematically coordinates risk assessment activities among the federal partners, this effort would go far in addressing the intent of our recommendation. Developing a plan that establishes a mechanism to systematically coordinate risk assessment activities and share the results of these activities among federal partners will also be an important and necessary step to fulfilling the agency’s oversight and coordination responsibilities.

TSA concurred with our second recommendation to include the results of available vulnerability and consequence assessment information in the upcoming revision to the Highway Modal Annex. In addition, TSA agreed to incorporate existing guidance developed by other federal and state highway infrastructure stakeholders, more clearly define security-related roles and responsibilities, establish a timeframe for its overall implementation and developing performance goals and measures. TSA stated that at the time of the drafting of the first iteration of the Highway Modal Annex, such vulnerability and consequence data was not available. TSA further stated that as the agency has expanded its CSR program, become more familiar with the stakeholder community security practices, and conducted much more detailed analyses of vulnerability and

mitigation tools, TSA has improved its ability to conduct more comprehensive risk assessments that address threat, vulnerability, and consequences. TSA further stated that while those elements were considered in the preparation of the initial Annex, the document itself did not adequately explain how they were incorporated into the resulting strategy, and that future Annex publications would better explain TSA's use of all three risk elements. TSA agreed that the agency is in the best position to provide strategy guidance, coordination and oversight in this area. TSA also agreed that implementation milestones and preparedness timeframes are appropriate for the Highway Modal Annex. However, TSA cautioned that any limitations on the stakeholder community's implementation strategies will be based on a lack of resources, and indicated that the National Strategy for Highway Bridge Security is intended to help responsible stakeholders find resources dedicated exclusively to address the security needs of their structures. TSA stated that it does not believe that direct regulation is appropriate for the stakeholder community accountable for highway structures because, based on its experience, TSA believes this to be an overwhelmingly responsible constituency that will be highly proactive given appropriate resources and guidance. However, until TSA provides the details of how it plans to address our recommendation that it incorporate available vulnerability and consequence information into the Highway Annex and take other steps to strengthen the Annex, it remains unclear whether TSA can demonstrate that the Highway Modal Annex provides highway infrastructure stakeholders with available useful information to identify and prioritize potential infrastructure security measures, enhances future planning efforts, clarifies roles and responsibilities, and provides accountability.

With regard to our third recommendation to develop a cost-effective mechanism to monitor the implementation of voluntary protective security measures on highway infrastructure assets identified as nationally critical, TSA agrees and stated that it is moving forward to identify a variety of mechanisms to monitor the voluntary security measures implemented with respect to critical highway structures. TSA stated that in fiscal year 2009, using funds made available specifically for this purpose for the first time since TSA was created, the agency will begin conducting individual vulnerability assessments on the nationally critical Tier 2 structures list. According to TSA, each assessment will be accompanied by a TSA-recommended approach to risk mitigation, and TSA will track the status of those recommendations on a periodic basis. TSA stated that its security partners will be kept informed of the progress of this effort. In addition, TSA stated its intention to clearly identify any to the implementation of

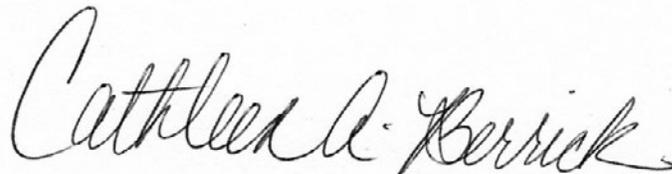
voluntary security measures and would assist stakeholders in executing identified measures. Our intention in making this recommendation is for TSA to have the tools to allow it to more effectively monitor the level of overall security preparedness of critical assets, help identify potential security gaps, establish protection priorities, and determine what, if any, additional measures may be needed to enhance highway infrastructure security. Despite TSA's stated plans, the agency has not indicated the frequency with which it plans to compile or analyze information on highway infrastructure operator's security practices for critical assets, nor did TSA provide a time frame for completing the asset specific vulnerability assessments or identify what mechanisms would be used to monitor their implementation of voluntary protective security measures on highway infrastructure assets identified as nationally critical. Taking such actions would be necessary to fully address the intent of this recommendation.

In addition, TSA noted that GAO has misstated or misinterpreted a key fact involving TSA's desire and intention to conduct individual vulnerability assessments on critical highway structures. TSA believes this misstatement significantly affects the findings of the report. TSA noted that the report indicates that TSA has either not decided whether to conduct such assessments or determined that they do not need to be done. Furthermore, TSA stated that it intends to conduct individual assessments on all bridge and tunnel properties that TSA has identified as critical, beginning in 2009. However, TSA did not indicate its desire to conduct these assessments, nor did it provide any documentation to support these plans, during the course of this review. Rather, throughout this review, TSA officials repeatedly told us that the resources associated with conducting individual vulnerability assessments of critical assets made it impractical to conduct such assessments. For this reason, TSA officials stated that they would utilize primarily a non asset-specific approach to conducting vulnerability assessments of the highway infrastructure sector, through the CSR program, and that the agency would rely on infrastructure owners and operators to conduct asset-level vulnerability assessments on highway assets. TSA officials did not make us aware of its plans to conduct individual vulnerability assessments of critical assets until the agency provided written comments on a draft of this report in January 2009. While we acknowledge TSA's stated intention to conduct individual vulnerability assessments on all critical highway infrastructure assets, we do not believe that the agency's recently reported plans to conduct these assessments affect the findings of this report because our discussion of TSA's efforts related to highway infrastructure vulnerability assessments was not used as the basis of any of the report's

recommendations. However, we have revised this report to clarify TSA's plans related to vulnerability assessments. DHS also provided technical comments and clarifications, which we have considered and incorporated 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 the Secretary of Homeland Security, the Secretary of Transportation, 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 have any further questions about this report, please contact me at (202) 512-3404 or berrickc@gao.gov. Contact points for our Office 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 VII.



Cathleen A. Berrick
Managing Director
Homeland Security and Justice Issues

Appendix I: Objectives, Scope and Methodology

Objectives

You asked us to assess the progress DHS has made in securing the nation's highway infrastructure. This report answers the following questions:

To what extent have federal entities assessed the risks to the nation's highway infrastructure and coordinated these efforts?

To what extent has DHS developed a risk-based strategy, consistent with applicable federal guidance and characteristics of an effective national strategy, to guide its highway infrastructure security efforts? and

What actions have government and highway sector stakeholders taken to secure highway infrastructure, and to what extent has DHS monitored the implementation of asset-specific protective security measures?

Scope and Methodology

To determine the extent that federal entities have assessed the risks to the nation's highway infrastructure and coordinated these efforts, we obtained and analyzed risk assessment data from DHS and DOT, comprised of various threat, vulnerability, and consequence related assessments for highway infrastructure assets.⁶³ We did not assess the quality of the assessments completed. We sought to determine the reliability of these data by, among other things, discussing methods of inputting and maintaining data with agency officials. On the basis of these discussions and our review of the processes used to collect the data, we determined that the data were sufficiently reliable for the purposes of this report. We interviewed DHS, DOT and selected state transportation, homeland security, and law enforcement officials, associations representing highway infrastructure owners and operators, and members of the Highway GCC and the Highway SCC, to discuss federal risk assessment efforts. Although the selected state transportation and homeland security officials perspectives cannot be generalized across the wider population of highway infrastructure owners and operators, because we selected these states based on characteristics including location, and input on states representing security programs in which minimal to more robust security measures were implemented, they provided us a broad overview of highway infrastructure asset security. We selected the associations that we spoke with based on input from TSA, FHWA, and industry stakeholders who identified the major associations representing highway infrastructure

⁶³ DHS determined that the risk assessment information is "For Official Use Only." As a result, the related data are not contained in this report.

owners and operators. To determine the extent to which TSA has used a risk management approach to guide decisions on securing highway infrastructure, we compared NIPP and TSSP requirements with TSA's efforts to implement such an approach. We focused on the strategic planning and risk assessment elements related activities of the NIPP management framework because DHS is early on in the process. The views reported include only those individuals we interviewed and are not necessarily representative of the views of others in those organizations. We also reviewed federal coordination and collaboration activities related to stakeholder efforts to assess and strengthen highway infrastructure security and compared them to GAO's recommended coordination practices. We also discussed with DHS, DOT and selected state transportation, homeland security, and law enforcement officials, associations representing highway infrastructure operators, and members of the Highway GCC, and the Highway SCC, the federal coordination and collaboration activities related to stakeholder efforts to assess and strengthen highway infrastructure security and compared them to the coordination requirements established in Homeland Security Presidential Directive-7, as well as GAO's recommended practices for effective collaboration. In addition, we analyzed TSA's actions regarding performance measurement with requirements in the Government Performance Results Act and GAO Standards for Internal Control in the Federal Government⁶⁴ regarding the use of use performance measurement. To obtain information on how threat information is shared and TSA's efforts to address threats, we met with officials from TSA's Highway Motor Carrier Division, TSA's OI, and HITRAC. Individuals from these offices provided documentation on DHS and DOT's threat assessment efforts. In addition, we met with officials from DOT's Office of Intelligence regarding the sharing of threat information.

To assess the extent to which DHS developed a risk-based strategy consistent with applicable federal guidance and characteristics of an effective national strategy to guide its highway infrastructure security

⁶⁴ Pub. L. No. 103-62, 107 Stat. 285 (1993); and 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 (FMFIA), provide the overall framework for establishing and maintaining internal control in the federal government. Also pursuant to FMFIA, 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.

efforts, we reviewed federal agency reports, guidelines, and infrastructure security studies sponsored by industry associations on using risk management, and interviewed DHS, and DOT officials and state and industry association highway infrastructure representatives regarding their use of risk management for protecting highway infrastructure. As the principal strategy for protecting the nation's highway infrastructure, we also analyzed TSA's Highway Modal Annex to determine how it aligned with the requirements set out in Executive Order 13416: Strengthening Surface Transportation Security. In addition, we assessed the extent to which the Highway Modal Annex contained the desirable characteristics for an effective national strategy that we have previously identified.⁶⁵

To identify the actions taken by government and highway sector stakeholders to enhance the security of highway infrastructure and assess the extent TSA has monitored the implementation of protective security measures implemented by stakeholders, we interviewed DHS, DOT, DOD, and selected state transportation, homeland security, and law enforcement officials, all major associations representing highway infrastructure operators, and members of the Highway GCC, and the Highway SCC. We also analyzed TSA, IP, and USCG vulnerability assessments of security practices at the state level and records of GCC and SCC meetings and stakeholder conferences. In addition, we selected 12 bridges and one tunnel to observe security measures implemented since September 11, 2001 and to discuss security-related issues with highway infrastructure owners and operators. We selected these assets based on characteristics including location, ownership, and criticality, and input on locations representing assets in which minimal to more robust security measures were implemented from TSA, DOT, and AASHTO⁶⁶. Because of the limited number of assets in our sample, and because the selected assets did not constitute a representative sample, the results of our observation and analysis cannot be generalized to the universe of highway infrastructure assets. However, we believe that the observations obtained from these visits provide us with a broad overview of highway infrastructure asset security. We also reviewed federal guidance and applicable laws and

⁶⁵ These characteristics were developed after our research found that there were no legislative or executive mandates identifying a uniform set of required or desirable characteristics for national strategies. For a more detailed discussion of these characteristics, see *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, [GAO-04-408T](#) (Washington, D.C: Feb. 3, 2004).

⁶⁶ AASHTO represents highway and transportation departments in the 50 states, the District of Columbia, and Puerto Rico.

regulations. In addition, we observed FHWA training programs and joint stakeholder conferences. We also reviewed DHS Science and Technology Directorate, TSA, DOT, AASHTO, and TRB documents to identify research and development efforts to improve highway infrastructure security. We also compared TSA's actions to obtain data on actions taken by highway infrastructure stakeholders to enhance security and to monitor implementation of those actions with criteria in GAO Standards for Internal Control in the Federal Government.⁶⁷

We conducted this performance audit from May 2007 through January 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.

⁶⁷[GAO/AIMD-00-21.3.1.](#)

Appendix II: Selected Laws and Federal Guidance Concerning the Security of Highway Infrastructure, 1996 to Present

Although there are no laws that specifically address highway infrastructure security or require highway infrastructure owners and operators to take certain security measures, a number of laws that generally address critical infrastructure protection and transportation security have been enacted. Similarly, the President has issued directives, and federal agencies have developed strategies, designed to coordinate the federal effort to ensure the security of critical infrastructure and transportation assets. The below table lists statutes, executive orders, presidential directives, and strategies that address critical infrastructure protection and transportation security.

Policy action	Date	Key elements
Executive Order 13010 ^a	July 1996	Established the President's Commission on Critical Infrastructure Protection (CIP) to study the nation's vulnerabilities to both cyber and physical threats. Identified the need for the government and the private sector to work together to establish a strategy for protecting critical infrastructures from physical and cyber threats.
Presidential Decision Directive 63	May 1998	Established CIP as a national goal and presented a strategy for cooperative efforts by government and the private sector to protect the physical and cyber-based systems essential to the minimum operations of the economy and the government. Superseded by HSPD-7 (see details on HSPD-7 below).
USA PATRIOT Act ^b	Oct. 2001	Established the National Infrastructure Simulation and Analysis Center (NISAC) to serve as a source of national competence to address critical infrastructure protection and continuity through support for activities related to counterterrorism, threat assessment, and risk mitigation.
Executive Order 13228 ^c	Oct. 2001	Established the Office of Homeland Security, within the Executive Office of the President, to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks. Established the Homeland Security Council to advise and assist the President with all aspects of homeland security and to ensure the coordination of homeland security-related activities of executive departments and agencies and effective development and implementation of homeland security policies.
Executive Order 13231 ^d	Oct. 2001	Established the President's Critical Infrastructure Protection Board, which was to recommend policies and coordinate programs for protection information systems for critical infrastructure.
Aviation and Transportation Security Act ^e	Nov. 2001	Created the Transportation Security Administration (TSA) and conferred upon TSA responsibility for security in all modes of transportation.
National Strategy for Homeland Security ^f	July 2002	Identified the protection of critical infrastructures and key assets as a critical mission area for homeland security. Specified 8 major initiatives for CIP, one of which specifically calls for the development of the NIPP.
Homeland Security Act of 2002 ^g	Nov. 2002	Created the DHS and assigned it the following CIP responsibilities: (1) developing a comprehensive national plan for securing the key resources

**Appendix II: Selected Laws and Federal
Guidance Concerning the Security of Highway
Infrastructure, 1996 to Present**

Policy action	Date	Key elements
		and critical infrastructures of the United States; (2) recommending measures to protect the key resources and critical infrastructures of the United States in coordination with other entities; and (3) disseminating, as appropriate, information to assist in the deterrence, prevention, and preemption of or response to terrorist attacks. Also provided for protection of voluntarily submitted information regarding the security of critical infrastructure.
The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets ⁿ	Feb. 2003	Identifies a set of goals and objectives and outlines the guiding principles that will underpin efforts to secure the infrastructures and assets vital to the nation's public health and safety, national security, governance, economy, and public confidence.
Exec. Order No. 13,286, 68 Fed. Reg. 10609 (Feb. 28, 2003).	Feb. 2003	Amended Executive Order 13231 but generally maintained the same national policy statement regarding the protection against disruption of information systems for critical infrastructures. Designated the National Infrastructure Advisory Council to continue to provide the President with advice on the security of information systems for critical infrastructures supporting other sectors of the economy through the Secretary of Homeland Security.
Homeland Security Presidential Directive 7	Dec. 2003	Superseded Presidential Decision Directive 63 and established that federal departments and agencies will identify and prioritize U.S. critical infrastructure and key resources and to protect them from terrorist attack. Defined roles and responsibilities for the DHS and sector-specific agencies to work with sectors to coordinate CIP activities. Established a CIP Policy Coordinating Committee to advise the Homeland Security Council on interagency CIP issues.
Homeland Security Presidential Directive 8	Dec. 2003	Directed DHS to coordinate the development of an all-hazards National Preparedness Goal that establishes measurable priorities, targets, standards for preparedness assessments and strategies, and a system for assessing the Nation's overall level of preparedness.
Intelligence Reform and Terrorism Prevention Act of 2004 ^l	Dec. 2004	Required the Secretary of Homeland Security to develop and implement a National Strategy for Transportation Security (NSTS) and modal security plans. Required the NSTS to include an identification and evaluation of the transportation assets that must be protected from attack or disruption, the development of risk-based priorities for addressing security needs associated with such assets, means of defending such assets, a strategic plan that delineates the roles and missions of various stakeholders, a comprehensive delineation of response and recovery responsibilities, and a prioritization of research and development objectives.
Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users ^l	Aug. 2005	Expanded security as a separate factor that must be addressed by statewide and metropolitan transportation plans by requiring that plans provide for consideration of projects and strategies that, among other things, will increase the security of the transportation system for motorized and non-motorized users.
National Strategy for Transportation Security	Sept. 2005	Outlines the Federal government's approach — in partnership with state, local and tribal governments and private industry — to secure the U.S. transportation system from terrorist threats and attacks, and prepare the Nation by increasing our capacity to respond if either occurs.

**Appendix II: Selected Laws and Federal
Guidance Concerning the Security of Highway
Infrastructure, 1996 to Present**

Policy action	Date	Key elements
Post-Katrina Emergency Management Reform Act ^k	Oct. 2006	<p>Expanded the purpose of the NISAC to include support for activities related to a natural disaster, act of terrorism, or other man-made disaster.</p> <p>Specified that the support must include modeling, simulation, and analysis of the systems and assets comprising critical infrastructure, in order to enhance preparedness, protection, response, recovery, and mitigation activities.</p> <p>Required any federal agency with critical infrastructure responsibilities under HSPD-7 to establish a relationship, including an agreement regarding information sharing, between such agency and the NISAC.</p>
National Infrastructure Protection Plan	June 2006	<p>Provided the framework and set the direction for implementing a coordinated, national effort. It provides a roadmap for identifying Critical Infrastructure/Key Resource assets, assessing vulnerabilities, prioritizing assets, and implementing protection measures in each infrastructure sector.</p>
Procedures for Handling Critical Infrastructure Information ^l	Sept. 2006	<p>Established procedures for federal, state, local, and tribal government agencies and contractors regarding the receipt, validation, handling, storage, marking, and use of critical infrastructure information voluntarily submitted to the DHS.</p>
Executive Order 13416 ^m	Dec. 2006	<p>Required the Secretary of Homeland Security to assess the security of each surface transportation mode and evaluate the effectiveness and efficiency of current surface transportation security initiatives.</p> <p>Imposed a deadline on the Secretary of Homeland Security to complete the Transportation Sector-Specific Plan (TSSP) and required the Secretary to develop modal annexes that addresses each surface transportation mode.</p>
Transportation Sector-Specific Plan (TSSP)	May 2007	<p>Establishes the transportation sector's strategic approach and related security framework.</p>
Highway and Motor Carrier Annex	May 2007	<p>Describes how the TSSP will be implemented in the Highway mode.</p>
Implementing Recommendations of the 9/11 Commission Act ⁿ	Aug. 2007	<p>Required the Secretary to establish and maintain a national database of each system or asset that the Secretary determines to be vital and the loss, interruption, incapacity, or destruction of which would have a negative or debilitating effect on economic security, public health, or safety, or that the Secretary otherwise determines to be appropriate for inclusion.</p> <p>Required the Under Secretary for Information Analysis and Infrastructure Protection, not later than 35 days after the last day of each fiscal year, including fiscal year 2007, to submit to the appropriate committees, for each sector identified in the NIPP, a report on the comprehensive assessments carried out by the Secretary of critical infrastructure and key resources, evaluating threat, vulnerability, and consequence.</p> <p>Required the Secretary, not later than 6 months after the last day of each fiscal year, to submit to the appropriate committees a report that details the actions of the federal government to ensure the preparedness of industry to reduce interruption of critical infrastructure and key resource operations during an act of terrorism, natural catastrophe, or other similar national emergency.</p> <p>Specified that the transportation modal security plans required under 49 U.S.C. § 114(t) must include threats, vulnerabilities, and consequences for aviation, railroad, ferry, highway, maritime, pipeline, public transportation, over-the-road bus, and other transportation infrastructure assets.</p> <p>Required that the National Strategy for Transportation Security include a 3- and 10-year budget for federal transportation security programs that will</p>

**Appendix II: Selected Laws and Federal
Guidance Concerning the Security of Highway
Infrastructure, 1996 to Present**

Policy action	Date	Key elements
		<p>achieve the priorities of the NSTS, methods for linking the individual transportation modal security plans and a plan for addressing intermodal transportation, and transportation modal security plans.</p> <p>Required the Secretary, in addition to submitting an assessment of the progress made on implementing the NSTS, to submit an assessment of the progress made on implementing the transportation modal security plans.</p> <p>Required that the progress reports include an accounting of all grants for transportation security, funds requested in the President's budget for transportation security, by mode, personnel working on transportation security, by mode, and information on the turnover in the previous year among senior staff working on transportation security issues.</p> <p>Required the Secretary, at the end of each fiscal year, to submit to the appropriate committees an explanation of any federal transportation security activity that is inconsistent with the NSTS.</p> <p>Required that the NSTS include the Transportation Sector-Specific Plan (TSSP) required by HSPD-7.</p> <p>Required the Secretary to establish a Transportation Security Information Sharing Plan, and specifies the contents of the plan</p> <p>Required the Secretary, not later than 150 days after enactment and annually thereafter, to submit to the appropriate committees a report containing the plan.</p> <p>Required the Secretary, to the greatest extent practicable, to provide public and private stakeholders with transportation security information in an unclassified format.</p> <p>Required the Secretary, in a semiannual report, to provide to the appropriate committees a report that includes the number of public and private stakeholders that were provided with each report, a description of measures that the Secretary has taken to ensure proper treatment and security for any classified information to be shared with stakeholders, and an explanation of the reason for the denial of information to any stakeholder that has previously received information.</p> <p>Required the Secretary to establish a National Transportation Security Center of Excellence to conduct research and education activities and to develop or provide professional security training.</p> <p>Provided for civil and administrative penalties for violations of transportation security regulations prescribed by the Secretary</p> <p>Authorized the Secretary to develop Visible Intermodal Prevention and Response (VIPR) teams to augment the security of any mode of transportation in any location in the United States.</p> <p>Authorized to be appropriated such funds as may be necessary to carry out this section for fiscal years 2007 through 2011.</p> <p>Authorized the Secretary to train, employ, and utilize surface transportation inspectors.</p> <p>Required the Secretary to establish a program to provide appropriate information that the Department has gathered or developed on the performance, use, and testing of technologies that may be used to enhance surface transportation security to surface transportation entities.</p> <p>Required the Inspector General of the DHS, not later than 90 days after enactment, to submit a report to the appropriate committees on the federal</p>

**Appendix II: Selected Laws and Federal
Guidance Concerning the Security of Highway
Infrastructure, 1996 to Present**

Policy action	Date	Key elements
		<p>trucking industry security grant program for fiscal years 2004 and 2005 that addresses the grant announcement, application, receipt, review, award, monitoring, and closeout process and states the amount obligated or expended under the program for fiscal years 2004 and 2005 for certain purposes.</p> <p>Required the Inspector General of the DHS, not later than 1 year after enactment, to submit a report to the appropriate committees that analyzes the performance, efficiency, and effectiveness of the federal trucking industry security grant program and the need for the program, using all years of available data, and that makes recommendation regarding the future of the program.</p>

Source: GAO analysis of documents listed above.

^aExec. Order No. 13,010, 61 Fed. Reg. 37,347 (July 15, 1996).

^b42 U.S.C. § 5195c.

^cExec. Order No. 13,228, 66 Fed. Reg. 51,812 (Oct. 8, 2001).

^dExec. Order No. 13,231, 66 Fed. Reg. 53,063 (Oct. 16, 2001).

^e49 U.S.C. § 114.

^fThe White House, Office of Homeland Security, National Strategy for Homeland Security.

^gPub. L. No. 107-296, §§ 201(d), 214, 116 Stat. 2135, 2145-47, 2152-55 (2002).

^hThe White House, The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.

ⁱ49 U.S.C. § 114(s).

^jPub. L. No. 109-59, § 6001(a), 119 Stat. 1144, 1839-57 (codified at 23 U.S.C. § 134, 135).

^k6 U.S.C. § 321.

^l6 C.F.R. §§ 29.1-29.9.

^mExec. Order No. 13,416, 71 Fed.Reg. 71,033 (Dec. 5, 2006).

ⁿPub. L. No. 110-53, 121 Stat. 266 (2007).

Appendix III: Examples of Selected Protective Security Measures that Could be Implemented by Asset Owners and Operators

Potential Countermeasures

Restrict physical access to critical systems and structures:

- Install fencing and other physical barriers to prevent access to critical bridge elements such as decks, piers, towers, and cable anchors.
- Utilize a full-time security officer to control access to restricted areas.
- Utilize security badges or other identification device to ensure access to restricted areas is properly controlled.
- Install locking devices on all access gates and utilize remote controlled gates where necessary.
- Eliminate parking under bridges or near critical structures.
- Protect tunnel ventilation intakes with barriers and install and protect ventilation emergency shut off systems.
- Utilize creative landscaping to increase standoff distance from critical areas.

Surveillance and detection efforts:

- Provide inspections to identify potential explosive devices, as well as increased or suspicious potential criminal activity.
- Display signs warning that the property is secured and being monitored.
- Install CCTV systems where they cannot be easily damaged or avoided while providing coverage of critical areas (to monitor activity, detect suspicious actions, and identify suspects).
- Install enhanced lighting with emergency backup.
- Install motion sensors or other intrusion detection systems.
- Clear overgrown vegetation to improve lines of sight to critical areas.

Security planning and coordination:

- Develop and implement a security plan that serves to identify critical systems and establishes procedures for their protection.
 - Provide emergency telephones to report incidents or suspicious activity.
 - Develop communication and incident-response protocols with applicable local, state, and federal law enforcement.
 - Review locations of trashcans or other storage areas that could be used conceal an explosive device and ensure they are not near critical areas.
 - Provide pass-through gates in concrete median barriers to enable rerouting of traffic and access for emergency vehicles.
 - Use of an advanced warning system, including warning signs, lights, horns, and pop-up barricades to restrict access after span failure (manually activated or activated by span failure detectors).
-

**Appendix III: Examples of Selected
Protective Security Measures that Could be
Implemented by Asset Owners and Operators**

Potential Countermeasures

Structural modifications:

- Shield the lower portions of cables on cable-stayed bridges and suspension bridges with protective armor to protect against damage from blast and fragmentation.
 - Increase the standoff distance and reduce access to critical elements with structural modifications (extending cable guide pipe length, moving guard rails, etc.).
 - Reinforce welds and bolted connections to ensure plastic capacity.
 - Use energy absorbing bolts to strengthen connections and reduce deformations.
 - Provide system redundancy to ensure alternate load paths exist should a critical structural element fail or become heavily damaged as a result of a terrorist attack.
-

Source: GAO analysis of data prepared by FHWA, IP, AASHTO, and TRB.

Appendix IV: Summary of Selected Federal and Non-Federal Research and Development Programs to Enhance Highway Infrastructure

Project Title	Description	Key Organization
Synthesis of surveillance and security technologies and development of info-sharing website.	This study is a synthesis of existing surveillance and security technologies to assist bridge owners in decision making. FHWA is also developing a website for infrastructure owners to access this information and interact with other owners on their effectiveness.	FHWA
Modeling and analysis of steel bridge towers subjected to blast loadings	This is a pooled fund experimental study to determine the effects of detonating explosives on steel bridge towers, develop and test retrofit strategies, and validate computer codes and modeling techniques.	FHWA
Bridge specific blast loading program	This study modified the Conventional Weapons Effects Program to provide a user friendly computer program for consistent definition of blast loadings on bridges titled the Bridge Explosives Loading (BEL) program.	FHWA
Blast testing of full scale, pre-cast, pre-stressed concrete girder bridges	FHWA is participating in this pooled fund study led by Washington State DOT to assess blast loadings and develop recommendations for possible mitigation measures that would harden this type of bridge blast damage.	WSDOT, FHWA
Blast resistant composite barriers	This study will characterize blast, fire and mechanical cutting –resistant material properties of available composite materials and the feasibility of producing improved properties through the use of nano-composites or other material modifications.	FHWA
Protective retrofit for small-diameter cables or thin-sectioned steel structural members	This study aims to establish performance requirements for a lightweight structural system for protecting small-diameter cables and thin-sectioned steel members against different attack methods.	FHWA
International Survey on Underground Transportation Systems in Europe	This survey identified European safety practices that can be used in the United States to improve safety. Specific practices and security strategies identified have been shared in a written report as well as outreach efforts to tunnel owners. As a secondary effort, FHWA developed a Load and Resistance Design Factor Guide for AASHTO which incorporated findings from the International Survey and has become the standard design methodology.	FHWA, AASHTO
Blast/Projectile Protection Project	This study includes basic research to understand the blast failure mechanisms of the most vital critical infrastructures such as dams, tunnels and bridges. In fiscal year 2007, the program developed a program plan and began physical testing and numerical modeling of blast effects on embankment dams and mitigation (hardening) measures for tunnels and bridge cables. In fiscal year 2008, the project began to evaluate blast effects and mitigation measures for dams, tunnels, and bridges. The amount of project funding targeted to bridge research was approximately \$3.0 million for fiscal year 2007 and fiscal year 2008. The amount dedicated to tunnels during this period was approximately \$1.9 million. However, an additional \$1.0 million of fiscal year 2007 Infrastructure/Geophysical funds were dedicated to tunnel research, bringing the total funding for tunnel research funding for to \$2.9 million.	DHS, Science and Technology Directorate
Infrastructure Blast Mitigation Project	This project is developing technologies to mitigate the explosive and damaging force from an IED. In fiscal year 2008, the project conducted tests and evaluation of prototype technologies to evaluate blast mitigation performance and performed proof-of-concept demonstrations. In fiscal year 2009, the project plans to begin to develop models to further determine the vulnerability of infrastructure, bridges, and tunnels to various explosive threats.	DHS, Science and Technology Directorate

Appendix IV: Summary of Selected Federal and Non-Federal Research and Development Programs to Enhance Highway Infrastructure

Project Title	Description	Key Organization
Rapid Mitigation and Recovery (for Critical Infrastructure) Project	This project is developing rapid mitigation and recovery technologies for critical infrastructure to limit damage and consequences and to more quickly resume normal operations. The project will investigate rapid response and recovery technologies in addition to conducting basic research for the most vital infrastructure assets, such as underwater tunnels, bridges, levees, and dams.	DHS, Science and Technology Directorate
Resilient Tunnel Project	This study seeks approaches to address critical vulnerabilities in U.S. transportation tunnels. Beginning in fiscal year 2007, this project surveyed concepts for tunnel protection, including studies on advanced materials for tunnel hardening and identification of an inflatable plug system, based on European technology, to limit the spread of fire. Further development of this system has continued in fiscal year 2008, with full completion and demonstration of a prototype inflatable plug currently scheduled for fiscal year 2010.	DHS, Science and Technology Directorate
Cooperative Research Program	<p>The following reports represent a sample of products completed at the request of the AASHTO Special Committee on Transportation Security:</p> <ul style="list-style-type: none"> • American Association of State Highway and Transportation Officials. Protecting America's Roads, Bridges, and Tunnels: The Role of State DOTs in Homeland Security. Project 20-59 (16). Washington, D.C., 2005. • Blue Ribbon Panel on Bridge and Tunnel Security. Recommendations for Bridge and Tunnel Security. Project 20-59 (3). Washington, D.C.: Federal Highway Administration, September 2003. • Transportation Research Board. A Self-Study Course on Terrorism-Related Risk Management of Highway Infrastructure. Project 20-59 (2). Washington, D.C., 2005. • Transportation Research Board. Disruption Impact Estimating Tool-Transportation (DIETT): A Tool for Prioritizing High-Value Transportation Choke Points. Project 20-59 (9). Washington, D.C., 2005. • Transportation Research Board. Guide to Making transportation tunnels safe and secure. Project 20-67. Washington, D.C., 2006. • Transportation Research Board. Guidelines for Transportation Emergency Training Exercises. Project 20-59 (18). Washington, D.C., 2005. • Transportation Research Board. National Needs Assessment for Ensuring Transportation Infrastructure Security. Project 20-59 (5). Washington, D.C., 2002. • Transportation Research Board. Responding to Threats: A Field Personnel Manuals. Project 20-59 (6). Washington, D.C., 2003. 	Transportation Research Board

Source: GAO analysis of information provided by DHS, FHWA, AASHTO, and TRB.

Appendix V: Comments from the Department of Homeland Security

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



**Homeland
Security**

January 21, 2009

Ms. Cathleen A. Berrick
Director, Homeland Security and Justice Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, D.C. 20548

Dear Ms. Berrick:

RE: Draft Report GAO-09-57SU, Highway Infrastructure: Federal Efforts to Strengthen Security Should Be Better Coordinated and Targeted on the Nation's Most Critical Highway Infrastructure (GAO Job Code 440633)

The Department of Homeland Security (DHS) appreciates the opportunity to review and comment on the draft report referenced above. The report contains two recommendations, one to the Department and another specifically addressed to the Transportation Security Administration. Department and Transportation Security Administration (TSA) officials agree with the recommendations.

TSA officials have already started to formulate implementation plans. The following response brings current any references made in the draft report to ongoing, developing, or maturing programs within TSA to ensure the integrity of any actions or decisions premised on this review. This report represents a snapshot of TSA initiatives as of the time of its compilation.

Although there is agreement with the recommendations, TSA officials believe that the U.S. Government Accountability Office (GAO) has misstated or misinterpreted a key fact and this misstatement significantly affects the findings of the report. The issue involves the TSA Highway and Motor Carrier (HMC) Division's desire and intention to conduct individual vulnerability assessments on critical highway structures. This report indicates that the TSA HMC Division has either not decided whether to conduct such assessments or has determined that they would not be done. TSA intends to conduct individual assessments on all bridge and tunnel properties that TSA had identified as "critical" and thus selected to occupy the DHS "Tier 2" structures list.

Recommendation 1:

The Secretary of Homeland Security establish a mechanism to systematically coordinate risk assessment activities and share the results of these activities among the federal partners.

www.dhs.gov

Response:

The Department agrees with the recommendation. TSA will have the lead in developing a sector coordinated risk assessment.

The function of “security risk assessment” has taken many forms under many agencies since the events of 9/11 and that a uniform and central system of assessment, data storage, and information sharing is critical to the effective implementation of terrorist mitigation tools in the future. In large part, TSA attributes the current state of coordination and information sharing to the enthusiasm of legacy U.S. Department of Transportation (USDOT) agencies to play a meaningful role in security immediately after the events of 9/11, the evolution of assignment of federal security responsibility through laws and policies, and the maturation processes of TSA and fellow DHS components. TSA recognizes, however, that it is responsible for all transportation security matters and intends to fulfill its leadership role in the highway infrastructure arena.

TSA is prepared to assume responsibility for all highway infrastructure security issues and will request of all DHS, USDOT and state or local governmental bodies that TSA become the repository for all risk-assessment models and data associated with this mode. Toward this goal, TSA has already convened representatives of both DHS and USDOT agencies to produce the document titled, *National Strategy for Highway Bridge Security*, which is currently under review by agencies and offices within both Departments. Once fully vetted, this document provides for appropriate participation and coordination of efforts by all federal agencies engaged in highway infrastructure security.

Recommendation 2:

The Assistant Secretary for the Transportation Security Administration, in consultation with the Highway Government Coordinating Council and the Highway Sector Coordinating Council should take the following two actions:

- (1) For the upcoming revision to the Highway Modal Annex:
 - (a) in addition to the results of threat assessment information, incorporate the results of available vulnerability and consequence assessment information into the strategy for securing highway infrastructure;
 - (b) consistent with Executive Order 13416 and desirable characteristics of an effective national strategy, identify existing guidance developed by other federal and state highway infrastructure stakeholders; indicate timeframes or milestones for its overall implementation for which entities can be held responsible; more clearly define security-related roles and responsibilities for highway infrastructure security activities for itself and other federal stakeholders, state and local government, and the private sector; establish a timeframe for developing performance goals and measures for monitoring the implementation of the Annex’s goals, objectives, and activities; and provide

more guidance on resource, investment, and risk management to help implementing parties allocate resources and investments according to priorities and constraints; and

- (2) develop a cost-effective mechanism to monitor the implementation of voluntary protective security measures on highway infrastructure assets identified as nationally critical.

Response:

TSA agrees with the recommendation. (1a) At the time of the drafting of the first iteration of the Highway Modal Annex, such vulnerability and consequence data was not available. As TSA has expanded its Corporate Security Review (CSR) program, personnel have become more familiar with stakeholder community security practices, and conducted much more detailed analyses of vulnerability and mitigation tools. As a result, TSA has improved its ability to conduct more comprehensive risk assessments that address threat, vulnerability, and consequences. While those elements were considered in the preparation of the initial Annex, the document itself did not adequately explain how they were incorporated into the resulting strategy. Future Annex publications will better explain TSA's use of all three risk elements.

TSA agrees that it is in the best position to provide strategy guidance, coordination, and oversight in this area. TSA also agrees that implementation milestones and preparedness timeframes are appropriate for the Highway Modal Annex, but cautions that limitations on this stakeholder community's implementation strategies will be based on lack of resources, not lack of enthusiasm. It is for that reason that the *National Strategy for Highway Bridge Security* document referenced in the response to Recommendation 1 seeks to help responsible stakeholders find resources dedicated exclusively to address the security needs of their structures.

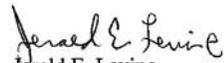
(1b) TSA has indicated to GAO that it does not believe that direct regulation is appropriate for the stakeholder community accountable for highway structures (largely state and local governments, quasi-government authorities and public corporations). Based on experience, TSA believes this to be an overwhelmingly responsible constituency that will be highly proactive given appropriate resources and guidance.

TSA does, however, agree with GAO's recommended actions for its motor carrier constituency. TSA is responsible for both motor carriers (e.g., trucks, buses) and highway structures (e.g., bridges, roads, tunnels). To be clear, the agency will provide guidance and consider regulations and compliance for the motor carrier segment of its stakeholder community but does not believe there is a need for regulation in the stakeholder community responsible for critical highway structures.

(2) TSA agrees and is moving forward to identify a variety of mechanisms to monitor the voluntary security measures implemented with respect to critical highway structures. In

Fiscal Year 2009, using funds made available specifically for this purpose, TSA will begin individual vulnerability assessments on its national critical Tier II structures list. Each assessment will be accompanied by a TSA-recommended approach to risk mitigation, and TSA will track the status of those recommendations on a periodic basis. TSA's security partners will be kept informed of progress. In addition, it is TSA's intention to clearly identify any hindrances to implementation and try to assist the stakeholder in executing identified measures.

Sincerely,



Jerald E. Levine
Director
Departmental GAO/OIG Liaison Office

MMcP

Appendix VI: GAO Contact and Staff Acknowledgments

GAO Contact

Cathleen A. Berrick, (202) 512-3404 or berrickc@gao.gov

Staff Acknowledgments

In addition to the contact named above, Steve Morris, Assistant Director, and Gary M. Malavenda, Analyst-in-Charge, managed this assignment. Jean Orland, Ryan Lambert, Susan Langley, and Dan Rodriguez made significant contributions to the work. Stan Kostyla and Chuck Bausell assisted with design, methodology, and data analysis. Linda Miller provided assistance in report preparation; Tracey King provided legal support; Nikki Clowers provided expertise on physical infrastructure issues; Sara Veale provided expertise on coordination and collaboration best practices; Elizabeth Curda provided expertise on performance management; and Pille Anvelt and Avrum Ashery developed the report's graphics.

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