United States Government Accountability Office

GAO

Report to Congressional Committees

November 2011

TRANSPORTATION SECURITY INFORMATION SHARING

Stakeholders Generally Satisfied but TSA Could Improve Analysis, Awareness, and Accountability

GAO-12-44

GAO
Accountability * Integrity * Reliability
Highlights

Highlights of GAO-12-44, a report to congressional committees

November 2011

TRANSPORTATION SECURITY INFORMATION SHARING

Stakeholders Generally Satisfied but TSA Could Improve Analysis, Awareness, and Accountability

Why GAO Did This Study

The U.S. transportation system, comprised of aviation, freight rail, highway, maritime, mass transit and passenger rail, and pipelines, moves billions of passengers and millions of tons of goods each year. Disrupted terrorist attacks involving rail and air cargo in 2010 demonstrate the importance of effective information sharing with transportation security stakeholders. The Transportation Security Administration (TSA) is the lead agency responsible for communicating security-related information with all modes. In response to the Implementing Recommendations of the 9/11 Commission Act of 2007, GAO assessed 1) the satisfaction of transportation stakeholders with the quality of TSA's transportation security information products, 2) satisfaction with mechanisms used to disseminate them, and 3) the extent to which TSA's roles and responsibilities are clearly defined. GAO surveyed 335 aviation, rail, and highway stakeholders (with an 82 percent response rate); reviewed agency planning documents; and interviewed industry associations, transportation stakeholders, and Department of Homeland Security officials. An electronic supplement to this report—GAO-12-67SP—provides survey results.

What GAO Recommends

GAO recommends that TSA, among other actions, (1) address stakeholder needs regarding the quality of analysis in and availability of its products, (2) increase awareness and functionality of its information sharing mechanisms, and (3) define and document TSA's information sharing roles and responsibilities. DHS concurred with GAO's recommendations.

View GAO-12-44. For more information, contact Stephen M. Lord at (202) 512-4379 or lords@gao.gov.

What GAO Found

Transportation stakeholders who GAO surveyed were generally satisfied with TSA's security-related information products, but identified opportunities to improve the quality and availability of the disseminated information. TSA developed a series of products to share security-related information with transportation stakeholders such as annual modal threat assessments that provide an overview of threats to each transportation mode—including aviation, rail, and highway—and related infrastructure. Fifty-seven percent of the stakeholders (155 of 275 who answered this question) indicated that they were satisfied with the products they receive. However, stakeholders who receive these products were least satisfied with the actionability of the information—the degree to which the products enabled stakeholders to adjust their security measures. They noted that they prefer products with more analysis, such as trend analysis of incidents or suggestions for improving security arrangements. Further, not all stakeholders received the products. For example, 48 percent (128 of 264) of the stakeholders reported that they did not receive a security assessment in 2010, such as TSA's annual modal threat assessment. Improving the analysis and availability of security-related information products would help enhance stakeholders' ability to position themselves to protect against threats.

Stakeholders who obtained security-related information through TSA's Web-based mechanisms were generally satisfied, but almost 60 percent (158 of 266) of stakeholders GAO surveyed had never heard of the Homeland Security Information Sharing Network Critical Sectors portal (HSIN-CS). DHS views HSIN as the primary mechanism for sharing security-related information with critical sectors, including transportation stakeholders. Forty-three percent of rail stakeholders, 28 percent of highway stakeholders, and 72 percent of aviation stakeholders—who consider TSA's aviation Web Boards as their primary information-sharing mechanism—had not heard of HSIN-CS. Among the 55 stakeholders that had logged on to HSIN-CS, concerns were raised with the ability to locate information using the mechanism. Increasing awareness and functionality of HSIN-CS could help ensure that stakeholders receive security information, including TSA products.

Defining and documenting the roles and responsibilities for information sharing among TSA offices could help strengthen information-sharing efforts. Officials from TSA's Office of Intelligence consider TSA's Transportation Sector Network Management offices to be key conduits for providing security-related information directly to stakeholders. However, officials from these offices differed in their understanding of their roles. For instance, officials told GAO that their role was to communicate policy and regulatory information, rather than threat-related information. While TSA officials look to the current Transportation Security Information Sharing Plan for guidance, it does not include key elements of the approach that TSA uses to communicate security-related information to stakeholders. For example, it does not describe the roles of TSA's Field Intelligence Officers, who facilitate the exchange of relevant threat information with local and private entities responsible for transportation security. Clearly documenting roles and responsibilities for sharing security-related information with transportation stakeholders could improve the effectiveness of TSA's efforts and help ensure accountability.

Contents

Tables

Figures

Abbreviations

DHS	Department of Homeland Security
FIO	Field Intelligence Officer
FSD	Federal Security Director
GCC	Government Coordinating Council
GRID	Global and Regional Intelligence Digest
HSIN	Homeland Security Information Network
HSIN-CS	Homeland Security Information Network Critical Sectors portal
HSIN-PT	Homeland Security Information Network public transit subportal
SCC	Sector Coordinating Council
TIN	Transportation Intelligence Note
TSA	Transportation Security Administration
TSA-OI	Transportation Security Administration Office of Intelligence
TSIR	Transportation Suspicious Incidents Report
TSISP	Transportation Security Information Sharing Plan
TSNM	Transportation Sector Network Management
TS-ISAC	Transportation Security Information Sharing and Analysis Center

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

November 21, 2011

Congressional Committees:

The U.S. transportation system comprises all modes of transportation (aviation, freight rail, highway, maritime, mass transit and passenger rail, and pipelines) and is an open, complex, and interdependent system that moves, distributes, and delivers billions of passengers and millions of tons of goods each year. The sheer size and capacity of the sector, which transports people, food, medicines, fuel, and other commodities vital to the nation's safety, security, and economic well being, makes it an attractive target for terrorists. Disrupted attempted terrorist activities in the fall of 2010—including a planned attack on the Washington, D.C., Metro system, the discovery of explosive devices in air cargo packages bound for the United States from Yemen, and information on threats to freight and passenger rail obtained after the death of Osama bin Laden—demonstrate the importance of effective information sharing with public and private transportation security stakeholders.

The Homeland Security Act of 2002 assigned the Department of Homeland Security (DHS) responsibility for sharing information with its federal, state, local, and private sector homeland security partners to assist in the prevention of and response to terrorist attacks.[1] The Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act) directed DHS to create a Transportation Security Information Sharing Plan (TSISP), which was first issued in July 2008 and most recently updated in December 2010 and is designed to establish a foundation for sharing transportation security-related information between public and private entities that have a stake in protecting the nation's transportation system.[2] While multiple DHS components are responsible for information sharing, the Transportation Security Administration (TSA) is the department lead on providing transportation security-related information to other DHS components and public and private stakeholders.

[1] Pub. L. No. 107-296, § 201(d)(9), 116 Stat. 2135, 2147 (2002).

[2] Pub. L. No. 110-53, § 1203(a), 121 Stat. 266, 383-85 (2007) (codified at 49 U.S.C. § 114(u)(2)).

Our prior work on information sharing with private and public security stakeholders has shown that information sharing continues to be a challenge for the federal government.[3] In January 2005, we designated establishing effective mechanisms for sharing terrorism-related information to protect the homeland a high-risk area because the government had continued to face challenges in analyzing and disseminating this information in a timely, accurate, and useful manner. We reported that information is a crucial tool in fighting terrorism and that its timely dissemination is critical to maintaining the security of our nation. This area remains on our high-risk list.[4] As a result of this designation, we monitor federal efforts to remove barriers to and better achieve information sharing. In addition, we have made a number of recommendations to DHS to strengthen this area and the agency has taken steps in response, such as expanding its efforts to share terrorism-related information with private sector entities and identifying state and local partners' information needs. The National Strategy for Information Sharing also discusses the need to improve information sharing, including enhancing the quantity and quality of specific, timely, and actionable information provided by the federal government to critical infrastructure sectors.[5] In 2010, we found that, while public transit agencies were generally satisfied with the security-related information they received, opportunities existed to streamline and reduce the volume of overlapping information they receive. We also found that some stakeholders were unaware of the information-sharing mechanisms available to them while others found them difficult to access or use. We recommended, among

[3] See, for example, GAO*, Information Sharing Environment: Better Road Map Needed to Guide Implementation and Investments,* GAO-11-455 (Washington, D.C.: July 21, 2011), *Public Transit Security Information Sharing: DHS Could Improve Information Sharing through Streamlining and Increased Outreach*, GAO-10-895 (Washington, D.C.: Sept. 22, 2010), *Information Sharing: Federal Agencies Are Sharing Border and Terrorism Information with Local and Tribal Law Enforcement Agencies, but Additional Efforts Are Needed*, GAO-10-41 (Washington, D.C: Dec. 18, 2009), *Information Sharing Environment: Definition of the Results to Be Achieved in Improving Terrorism-Related Information Sharing Is Needed to Guide Implementation and Assess Progress*, GAO-08-492 (Washington, D.C.: June 25, 2008), and *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information*, GAO-06-385 (Washington, D.C.: Mar. 17, 2006).

[4] Every 2 years, GAO provides Congress with an update on its High-Risk Program, which highlights major problems that are at high risk for waste, fraud, abuse, mismanagement, or in need of broad reform. There are 31 areas on GAO's High-Risk list. GAO, *High Risk Series: An Update*, GAO-11-278 (Washington, D.C.: February 2011).

[5] *National Strategy for Information Sharing* (Washington, D.C.: October 2007).

other things, for DHS and TSA to assess opportunities to streamline mechanisms and to improve the awareness, use, and access to these mechanisms among public transit stakeholders.[6]

Section 1203 of the 9/11 Commission Act directed us to conduct a survey of the satisfaction of recipients of transportation security-related information disseminated under the TSISP.[7] In response to this mandate, we assessed the satisfaction of recipients of transportation security-related information within the aviation, passenger and freight rail, and highway modes.[8] Specifically, our report addresses the following questions:

- To what extent are transportation stakeholders satisfied with the quality of TSA's transportation security-related information products?
- To what extent are stakeholders satisfied with the mechanisms used to disseminate these products?
- To what extent has TSA defined its roles and responsibilities for sharing security-related information with stakeholders?

To assess the extent to which stakeholders are satisfied with the security-related information products that they receive from TSA and the mechanisms by which they access them, we surveyed transportation stakeholders from the aviation, freight and passenger rail, and highway modes. The survey was conducted in April and May 2011 and included 335 stakeholders; we received responses from 275 stakeholders (82 percent of those surveyed). Specifically, the survey was sent to security officials at commercial passenger air carriers, Category X and I commercial airports, air cargo carriers, Amtrak, Class I freight rail carriers, short line and regional railroads that carry toxic inhalation hazards or operate in high-threat urban areas, and state departments of

[6] GAO-10-895. DHS and TSA concurred with our recommendations. Actions being taken to implement these recommendations are discussed in this report.

[7] Pub. L. No. 110-53, § 1203(a), 121 Stat. 266, 383-85 (2007) (codified at 49 U.S.C. § 114(u)(7)).

[8] We conducted a similar review on the satisfaction of public transit stakeholders in 2010 and therefore, did not assess the satisfaction of public transit stakeholders in this review. See GAO-10-895.

transportation or emergency management.[9] We sent the survey to the entire known population of organizations; no sampling was conducted. While the survey responses cannot be used to generalize the opinions and satisfaction of all transportation stakeholders as a whole, the responses provide data for our defined population. The survey document and counts of responses received for each question are reproduced in an electronic supplement we are issuing concurrent with this report—GAO-12-67SP. To obtain additional narrative and supporting context from stakeholders, survey respondents were given multiple opportunities to provide additional open-ended comments throughout our survey. Additional information was obtained from interviews with industry associations, TSA and DHS officials, and 18 individual stakeholders who were selected based on their geographic location and mode of transportation. While the opinions expressed in the interviews are nongeneralizable to all stakeholders or modes of transportation, they provided important perspective to our analysis. We also reviewed documents and plans that describe recommended practices for effective information sharing.

To assess the extent to which TSA has defined its roles and responsibilities for sharing security-related information with stakeholders, we interviewed officials from TSA's Office of Intelligence (TSA-OI) and officials from the Commercial Airline, Commercial Airport, Air Cargo, Freight Rail, and Highway and Motor Carrier units within the Office of Transportation Sector Network Management (TSNM) on the functions they perform in information sharing.[10] We compared the practices described by these officials, industry associations, and individual stakeholders to those described in the TSISP and other DHS and federal

[9] Category X airports represent the nation's largest and busiest airports as measured by the volume of passenger traffic and are potentially attractive targets for criminal and terrorist activity. TSA classifies the nation's airports into one of five categories (X, I, II, III, and IV) based on various factors such as the number of takeoffs and landings annually, the extent of passenger screening at the airport, and other security considerations. In general, Category X airports have the largest number of passenger boardings and Category IV airports have the smallest. As defined by revenue, for 2009, Class I railroads are freight rail carriers having an operating revenue of $379 million or more. Our survey responses represent each of the stakeholder groups described but are not generalizable to entire modes of transportation such as aviation, rail, and highways.

[10] In September 2011, TSA announced that, as part of a headquarters realignment, TSA-OI will become part of a new Office of Intelligence and Analysis and the Office of TSNM will transition to the Office of Security Policy and Industry Engagement.

plans that describe effective practices for information sharing. Appendix I provides more details about our objectives, scope, and methodology.

We conducted this performance audit from May 2010 through November 2011 in accordance with generally accepted government auditing standards.[11] Generally accepted government auditing standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

The Aviation and Transportation Security Act, enacted in November 2001, assigned TSA responsibility for security in all modes of transportation, which include aviation, maritime, mass transit, highway and motor carrier, freight rail, and pipeline.[12] The act included requirements for deploying a federal screening workforce at airports and screening all passengers and property transported from or within the United States on commercial aircraft.[13] While TSA has a more direct role in ensuring the security of the aviation mode through its management of a passenger and baggage screener workforce that inspects individuals and their property to deter and prevent an act of violence or air piracy, TSA has a less direct role in securing other modes—such as freight rail and highway and motor carrier—in that it generally establishes voluntary standards, conducts inspections, and provides recommendations and advice to owners and operators within those modes. Responsibility for securing these modes is shared with other federal agencies, state and local governments, and the private sector. However, TSA has responsibility for receiving, assessing,

[11] We reported preliminary results from our ongoing work on challenges in sharing information with transportation stakeholders in September and June 2011. *GAO, Department of Homeland Security: Progress Made and Work Remaining in Implementing Homeland Security Missions 10 Years after 9/11,* GAO-11-881 (Washington, D.C.: Sept. 7, 2011), and *Rail Security: TSA Improved Risk Assessment but Could Further Improve Training and Information Sharing,* GAO-11-688T (Washington, D.C.: June 14, 2011).

[12] Pub. L. No. 107-71, § 101(a), 115 Stat. 597 (2001) (codified as amended at 49 U.S.C. § 114(d)).

[13] For purposes of this report, “commercial aircraft” refers to a U.S. or foreign-based air carrier operating under TSA-approved security programs with regularly scheduled passenger operations to or from a U.S. airport.

and distributing intelligence information related to transportation security in all modes and assessing threats to the transportation system.

Within TSA, the Office of TSNM is responsible for setting policy for all modes of transportation.[14] For example, the Mass Transit TSNM office develops strategies, policies, and programs to improve transportation security including operational security activities, training exercises, public awareness, and technology. TSA-OI receives intelligence information regarding threats to transportation and aims to disseminate it, as appropriate, to officials in TSA, the federal government, state and local officials, and to industry officials with transportation responsibilities. Although it is not an intelligence generator, the office receives and assesses intelligence from within and outside of the intelligence community to determine its relevance to transportation security.[15] Sources of information outside the intelligence community include other DHS components, law enforcement agencies, and owners and operators of transportation systems. TSA-OI also reviews suspicious activity reporting by Transportation Security Officers, Behavior Detection Officers, and Federal Air Marshals.[16] TSA-OI has deployed Field Intelligence Officers (FIO) throughout the United States to provide additional

[14] TSA TSNM divisions include Freight Rail, Highway and Motor Carriers, Port and Intermodal, Mass Transit, Pipelines, Air Cargo, Commercial Aviation, and General Aviation.

[15] The U.S. intelligence community is a coalition of 17 agencies and organizations within the executive branch that work both independently and collaboratively to gather the intelligence necessary to conduct foreign relations and national security activities. Its primary mission is to collect and convey the essential information the President and members of the policymaking, law enforcement, and military communities require to execute their appointed duties.

The 17 member agencies are: Air Force Intelligence, Army Intelligence, Central Intelligence Agency, Coast Guard Intelligence, Defense Intelligence Agency, Department of Energy, Department of Homeland Security, Department of State, Department of the Treasury, Drug Enforcement Administration, Federal Bureau of Investigation, Marine Corps Intelligence, National Geospatial-Intelligence Agency, National Reconnaissance Office, National Security Agency, Navy Intelligence, and the Office of the Director of National Intelligence.

[16] Transportation Security Officers inspect baggage and cargo and screen passengers to detect and prevent potentially dangerous objects from being transported into secure areas or onto aircraft. Behavior Detection Officers examine passenger behaviors to identify those who might pose a security threat. Federal Air Marshals serve as the primary law enforcement entity within TSA and are deployed on flights to protect air passengers and crew.

intelligence support to Federal Security Directors (FSD) who are responsible for providing day-to-day operational direction for federal security at airports—and their staffs. In addition, the FIOs serve as liaisons with state, local, and tribal law enforcement officials and intelligence fusion centers.[17] TSA-OI disseminates security information through security-related information products including reports, assessments, and briefings. These products are also shared with intelligence community members and other DHS organizations. Table 1 describes TSA's primary security-related information-sharing products. TSA is one of several sources of security-related information for transportation stakeholders. These stakeholders may also receive information from other federal agencies such as the Federal Bureau of Investigation (FBI), Department of Defense, and Department of Transportation, as well as, among others, state and local fusion centers and industry associations.

Table 1: Primary TSA Information-sharing Products

Product	Description	Frequency
Reports	The Transportation Intelligence Note (TIN) aims to provide additional information or analysis on a single specific issue/topic, or provides situational awareness of an ongoing or recent event/incident. TIN lengths vary–from one to five pages–and can be produced at the classified and unclassified levels. TINs are regularly distributed to TSA officers and transportation security partners with more than 90 being produced in one 6-month period.	As needed
	The Transportation Suspicious Incidents Report (TSIR) provides a summary of incidents and open source reporting emerging in the last 7 to10 days including reports of suspicious activities and surveillance directed against transportation modes. It provides information on threats, significant airport and aircraft incidents, terrorist groups, security trends and new technologies, and intelligence community and Law Enforcement advisories. Until August 2011, the TSIR was produced weekly at the unclassified level and was made available to transportation security professionals through e-mail and secure web-based portals. In August 2011, TSA phased out the TSIR and replaced it with the Global and Regional Intelligence Digest (GRID).[a]	Weekly

[17] A fusion center is generally a collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity.

Product	Description	Frequency
Assessments	According to TSA-OI, assessments typically include analysis of the threat, a discussion of potential actors, targets, and tactics, and may include an outlook or review of potential countermeasures or vulnerabilities. They may also include speculative or predictive analysis, as well as appendices providing detailed charts or supporting information. These documents are produced at the classified and unclassified levels. TSA-OI produces various assessments, including:	
	• modal threat assessments (aviation, freight rail, pipeline, highway, mass transit, ferries);	Annually
	• special event threat assessments (transportation focus only, usually covers National Special Security Events);	As needed
	• tactics, techniques, and procedures assessments; and	As needed
	• current airport threat assessments (threat information for various classes of airports across the United States).	Semiannually
Briefings	According to TSA-OI officials, TSA may share transportation security-related information, including details on threats, vulnerabilities, and suspicious activities with transportation stakeholders during unclassified or classified briefings. These briefings may be provided on an as-needed basis to individual security professionals, public and private stakeholders, local and regional groups, or more regularly to entire industries at forums such as trainings, workshops, and conferences. These briefings may also be conducted at TSA headquarters, at other secure locations, over a secure phone line, or via video or teleconference. For example, TSA regularly briefs senior security staff at a passenger air carrier every 3 months at TSA headquarters covering areas of international operation.	As needed

Source: GAO analysis of information provided by the TSA Office of Intelligence.

Note: This list does not include all of TSA's information-sharing products, but rather those identified by TSA and transportation stakeholders as the primary products produced by TSA.

[a] According to TSA-OI, the GRID aims to provide monthly analyses of operational reporting on suspicious activities and surveillance directed against all transportation modes. While the content includes information similar to the TSIR, the GRID also shows trend analysis, detailing specific suspicious incidents both regionally and globally.

TSA uses multiple mechanisms to distribute these products. Table 2 describes some of the mechanisms that TSA uses. Other mechanisms that transportation stakeholders may use to obtain security-related information include those operated by regional, state, and local entities such as law enforcement agencies and emergency operations centers, as well as industry-sponsored mechanisms such as the Association of American Railroads' Railway Alert Network, among others.

Table 2: TSA Information-sharing Mechanisms

Mechanism	Description
Homeland Security Information Network (HSIN)	HSIN is a web-based platform operated by DHS to facilitate Sensitive But Unclassified (SBU) information-sharing and collaboration between federal, state, local, tribal, and private sector entities. DHS describes HSIN as its primary information-sharing mechanism. HSIN is made up of a growing network of communities, called Communities of Interest. These communities are organized by state organizations, federal organizations, or mission areas such as emergency management, law enforcement, critical sectors, and intelligence. HSIN Critical Sectors (HSIN-CS) is the portal designated to provide security-related information for critical infrastructure sectors and includes specific subportals for individual modes of transportation such as public transit, freight and passenger rail, and highway and motor carriers. In March 2010, TSA-OI implemented its Transportation Security Information Sharing and Analysis Center (TS-ISAC), now called TSA Intel on HSIN. TSA initiated the page to serve as a venue to obtain TSA-OI reports and documentation, such as SBU intelligence products and other documents from other transportation security partners and stakeholders. Users must have a HSIN password to access TSA Intel on HSIN. Once access is obtained, users can set up alerts to be notified when a new document has been posted. According to TSA, while once considered the one-stop shop for TSA security-related information products, this page is no longer intended to be the only avenue for dissemination of intelligence products.
E-mail alerts	As a part of its information-sharing efforts, TSA's Office of Intelligence and Transportation Sector Network Management occasionally disseminate e-mails to transportation organizations that include "unclassified" and "Sensitive But Unclassified" security-related information. This TSA mechanism is intended to provide transportation stakeholders with information such as suspicious incident and situational awareness reports.
TSA's Aviation Web Boards	The Aviation Web Boards are websites devoted to aviation security-related information. Access to the Aviation Web Boards can only be obtained through TSA. In addition to regulatory and policy documents, TSA posts security-related information on the Web Boards with the expectation that stakeholders are viewing new information daily. There are designated Web Boards for divisions of aviation operators including airports, passenger air carriers, and air cargo carriers.

Source: GAO summary of information provided by DHS.

Stakeholders Generally Satisfied with TSA Information Products but Identified Opportunities to Improve Quality and Availability

Stakeholders Were Generally Satisfied with Information, although Satisfaction Varied by Sector

Because the private sector owns and operates the majority of infrastructure and resources that are critical to our nation's physical and economic security, it is important to ensure that effective and efficient information-sharing partnerships are developed with these private sector entities. Both the TSISP and DHS's Information Sharing Environment Implementation Plan emphasize the importance of two-way information sharing between government and industry through a framework that communicates actionable information on threats and incidents. In support of this endeavor, TSA is responsible for receiving, assessing, and distributing intelligence information related to transportation security and acting as the primary liaison for transportation security to the intelligence and law enforcement communities.[18]

TSA has developed security-related information products as part of its efforts to share security-related information with transportation stakeholders. Our 2011 survey results indicate general satisfaction among transportation stakeholders who received these products across each mode of transportation, but satisfaction varied by transportation

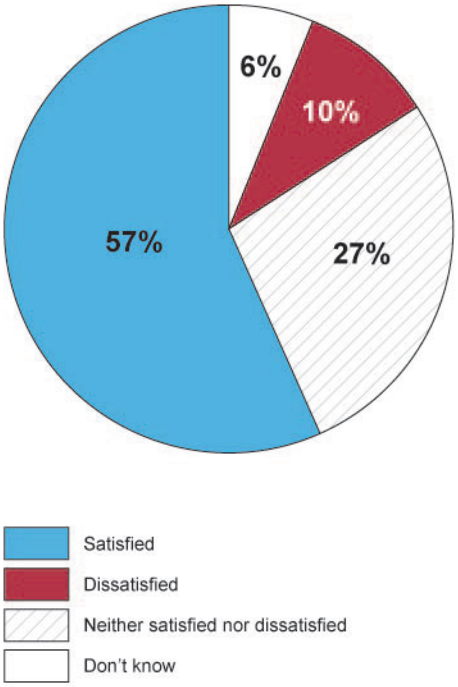
[18] See 49 U.S.C. § 114(f)(1), (5).

sector.[19] As highlighted in figure 1, 57 percent (155 of 275) of all stakeholders who responded to our survey question concerning overall satisfaction were satisfied with the security-related information they received, while approximately 10 percent (27 of 275) were dissatisfied.[20]

[19] Survey respondents were asked to rate their satisfaction using the following terms: “very satisfied”, “somewhat satisfied”, “neither satisfied nor dissatisfied”, “somewhat dissatisfied”, “very dissatisfied”, and “don’t know”. We use the term “satisfied” to describe agencies that indicated they were either “very satisfied” or “somewhat satisfied” with the information they received. Similarly, we use the term “dissatisfied” to describe agencies that indicated they were either “very dissatisfied” or “somewhat dissatisfied” with the information they received. It should be noted that because satisfaction and dissatisfaction are not the only possible responses, when we report that 57 percent of respondents reported being satisfied, for example, that does not necessarily mean that 43 percent were dissatisfied. We describe results for seven different sectors: commercial passenger air carriers, commercial airports, air cargo carriers, Amtrak, Class I freight rail carriers, short line and regional railroads, and highways.

[20] Although 275 transportation stakeholders responded to our survey, not all respondents provided answers to every question. The survey instrument and complete counts of responses received for each question can be found in an electronic supplement we are issuing concurrent with this report—GAO-12-67SP.

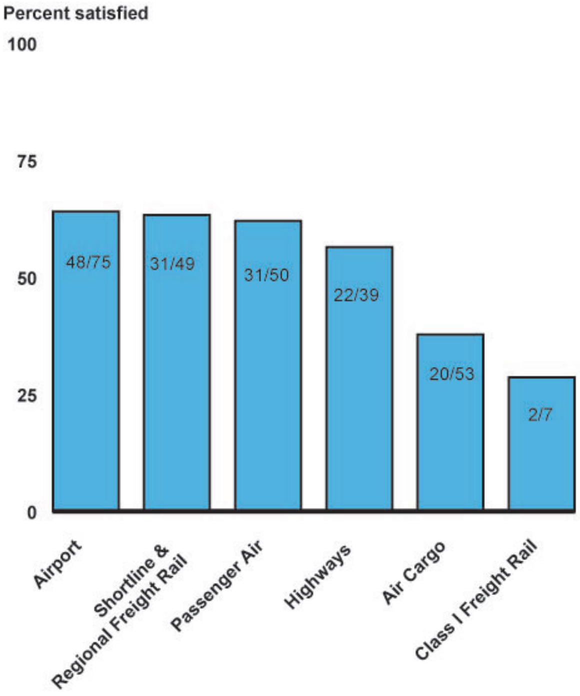
Figure 1: Stakeholder Satisfaction with All TSA Security-related Products and Briefings



Source: GAO analysis of survey responses.

Survey results regarding satisfaction with security-related information products and briefings across transportation sectors indicate that respondents from five of the seven sectors we surveyed were satisfied. However, less than half of all respondents from both the air cargo (20 of 53) and class I rail (2 of 7) sectors respectively, were satisfied with TSA's products, as shown in figure 2.

Figure 2: Percent of Stakeholders Satisfied with TSA's Products and Briefings by Sector



Source: GAO analysis of survey responses.

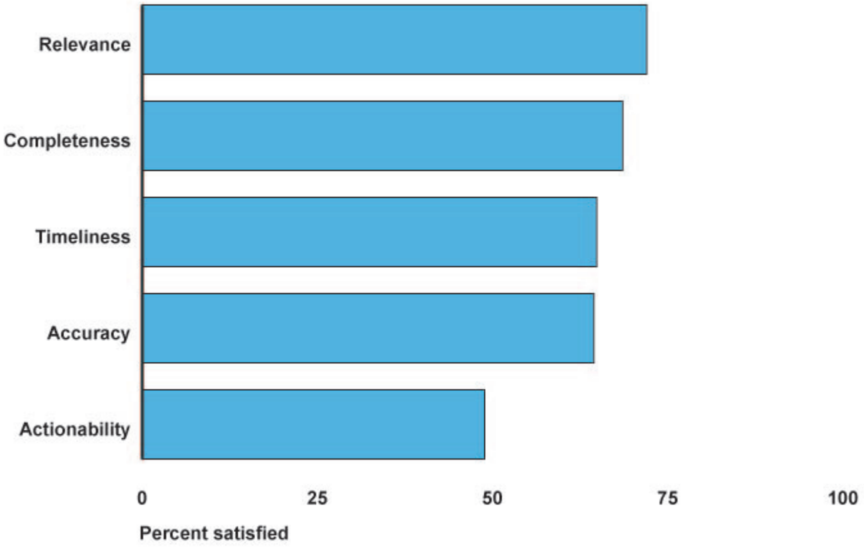
Note: Because our survey instructions stated that we would not attribute any responses to a particular organization and would not share individually identifiable responses, Amtrak results are not represented in figure 2. Amtrak was the only passenger rail carrier included in our survey. Amtrak's responses are aggregated with Class I and Short Line and Regional Freight stakeholders when we refer to the rail mode. (Other passenger rail carriers were surveyed as part of our September 2010 report on public transportation security information-sharing efforts; see GAO-10-895.)

We also asked survey respondents about their satisfaction with the transportation security-related information they received or obtained from a variety of other sources including the industry associations, FBI, and security consultants, among others. As discussed earlier, other organizations also provide transportation security information to state and local transportation agencies. Stakeholders were generally satisfied with the information from these other sources. For example, stakeholder satisfaction among respondents that received information from the industry associations, FBI, and security consultants was 81 percent (165 of 203), 69 percent (96 of 139), and 51 percent (52 of 102) respectively.

Stakeholders Identified Opportunities for Improving Product Actionability

Stakeholder satisfaction with TSA products was measured both in terms of overall satisfaction with all products combined, as well as across five separate dimensions of quality—accuracy, actionability, completeness, relevance, and timeliness for each product type. Regarding these specific dimensions, more stakeholders were satisfied with the relevance and completeness of these products, whereas fewer stakeholders were satisfied with the actionability of TSA's products, as shown in figure 3.

Figure 3: Average Percent of Stakeholders Satisfied with TSA Products and Briefings by Quality Dimension



Source: GAO analysis of survey responses.

Note: Not all stakeholders received each of the three products (reports, assessments, and briefings) represented by this figure; therefore survey respondents could have expressed their satisfaction with one, two, or all three of these products. This figure represents the average percent satisfaction of each quality dimension across each of the product types mentioned in our survey. The percentages averaged did not vary by more than 3 percentage points.

As shown in figure 3, an average of 72 and 69 percent of stakeholders we surveyed reported being satisfied with the relevance and completeness, respectively, of these products, compared to an average of 59 percent satisfaction with the actionability of this information. For the purposes of the survey, actionability was defined as the degree to which TSA's security-related information products enabled stakeholders to make adjustments to their security measures, if such a change was warranted. In open-ended comments included in our survey, stakeholders from each of the sectors stated that actionable information also includes analysis of trends, practices, and probability that would allow them to adjust their security measures as appropriate.

For example, of the 53 air cargo stakeholders that completed our survey, 6 provided open-ended comments in our survey that TSA provides very little security-related information to their industry concerning unscheduled air carriers such as on-demand cargo operations. These stakeholders stated that the information they receive is usually related to either large cargo companies like FedEx and UPS or passenger air carriers. While only one Class I rail survey respondent reported being dissatisfied with the security-related information their organization receives, five of the seven Class I respondents cited concerns with the lack of analysis associated with the information they receive from TSA.[21] For example, one Class I respondent suggested TSA increase incident analysis and provide more detail on various terrorist approaches and how these methodologies may impact freight rail. According to this respondent, more rail-specific analysis would assist their industry with developing current countermeasures to be as effective as possible against mitigating potential threats.

Open-ended comments collected in our survey from 18 of the 275 stakeholders provided additional context about actionability. For example, 6 aviation stakeholders reported that informational reports, specifically the TSIRs—which TSA phased out and replaced with the more regionally focused GRID in August 2011—would be more beneficial if they provided actionable information or additional guidance that would allow the stakeholders to adjust security measures or take other necessary actions to improve their security postures, and also identify ongoing trends to various sectors.[22] One passenger air carrier official commented that these reports are ambiguous—often leaving him wondering what information may affect his airline and what changes should or could be made to directly counter specific threats. Additionally, 8 of the 16 aviation and

[21] The other four Class I freight rail survey respondents that cited concerns with the lack of analysis were neither satisfied nor dissatisfied with the security information that they receive.

[22] TSA officials stated that the GRID will provide a better opportunity for TSA to provide an analytical summary of law enforcement and open source reporting emerging in the last 30 days, including information on threats, significant airport and aircraft incidents, terrorist groups, security trends and new technologies, and intelligence and law enforcement advisories.

freight rail stakeholders we interviewed stated that TSA's security-related information products lacked actionable analysis and did not contain information that would allow them to take any specific actions. Also, 7 of the 18 stakeholders we interviewed across each of the three modes commented that opportunities exist for TSA to increase incident analysis and provide more detail on pre-attack planning as well as the trends identified in various terrorist attempts and how these may impact their industry. Our previous work on information sharing highlights continuing challenges that DHS faces in providing actionable information to its stakeholders. For example, we previously reported that most information-sharing and analysis centers established to share information with stakeholders from critical sectors have expressed concerns with the limited quantity of information and the need for more specific, timely, and actionable information from DHS and/or their sector-specific agencies.[23]

According to DHS, the federal government is uniquely positioned to help inform critical security investment decisions and operational planning as private sector operators generally look to the government as a source of security-related threat information. However, we found that a lack of actionable TSA data has led stakeholders to rely on other sources for relevant security-related information. Of the 275 stakeholders who completed our survey, 203 reported receiving security-related information from other sources. Additionally, Amtrak officials told us that they have contracted with intelligence analysts at Spectel to monitor open and sensitive data sources for rail-related security material. The analysts produce a weekly report called Railwatch that, according to these officials, helps them develop tactics to defend against terrorist activity. Amtrak officials told us that these analysts also work closely with government agencies, including fusion centers, to develop and share information that they described as much more rail-centric than the daily security information that DHS makes available to them. TSA officials noted that aviation stakeholders may receive security directives that outline required steps for enhancing security. They stated that providing prescriptive actionable intelligence is challenging as there is not always information available. However, they recognized the need to provide this information to stakeholders when available and to improve the analysis provided in their products.

[23] GAO, *Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors*, GAO-04-780 (Washington, D.C.: July 9, 2004).

Some Transportation Stakeholders Did Not Receive TSA's Security-related Information Products

According to the TSISP, TSA's information-sharing products represent an important part of its efforts to establish a foundation for sharing security-related information with all appropriate public and private transportation stakeholders. We have previously reported that information is a crucial tool in fighting terrorism and that its timely dissemination is critical to maintaining the security of our nation.[24] When stakeholders are provided with a comprehensive picture of threats or hazards and participate in ongoing multidirectional information flow, their ability to make prudent security investments and develop appropriate resiliency strategies is substantially enhanced.[25] According to the TSISP, two-way information sharing between government and industry is one of the goals of maintaining the security of our nation's transportation system.[26]

However, some of TSA's stakeholders are not receiving these products. We surveyed stakeholders who TSA had identified as points of contact who should receive TSA security-related information products. As shown in figure 4, approximately 18 percent (48 of 266 stakeholders who provided responses to this question) of the transportation stakeholders we surveyed reported that they did not receive TSA's transportation security-related information reports, 34 percent (91 of 271) reported that they did not receive a TSA briefing, and approximately 48 percent (128 of 264) reported that they did not receive TSA's assessments in 2010.[27] Among the rail stakeholders we surveyed, approximately 11 percent (6 of 57) reported not receiving any security-related information reports while 32 percent (18 of 56) reported they did not receive an assessment from TSA.

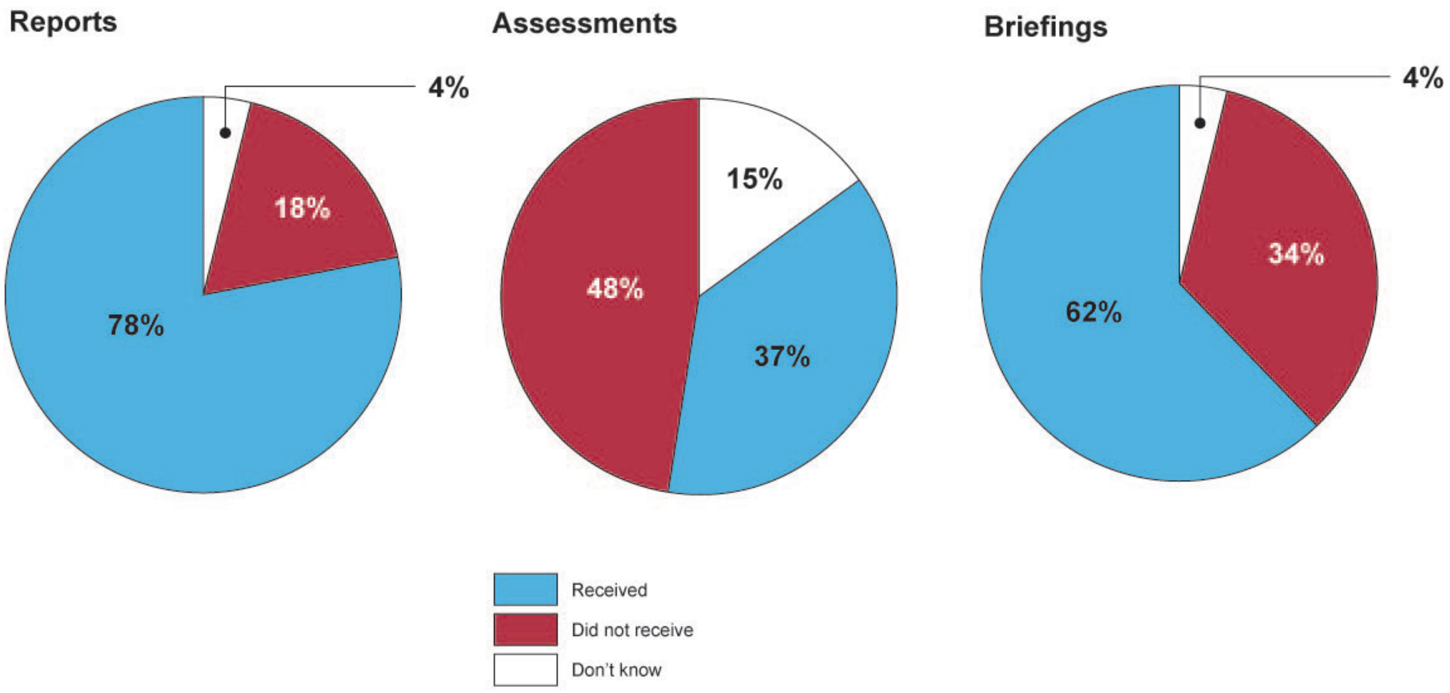
[24] GAO, *High Risk Series: An Update*, GAO-05-207 (Washington, D.C.: January 2005).

[25] DHS, *National Infrastructure Protection Plan* (Washington, D.C.: June 2006).

[26] Other goals outlined in the TSISP include: Effective and Efficient Processes, Trusted Partnerships, Right Information-Right People-Right Time, and Protecting Privacy and Civil Liberties.

[27] Note that briefings can include scheduled presentations at conferences as well as conference calls and meetings.

Figure 4: Stakeholders' Receipt of TSA Security-related Information Products



Source: GAO analysis of survey responses.

Approximately 78 percent (207 of 266) of the survey respondents across all modes reported receiving TSA reports.[28] However, the number of transportation security stakeholders who received TSA's assessments and briefings varied by mode.[29] Survey responses also indicated that TSA is the primary, but not only, source for these products. For example, 36 percent (49 of 207) of survey respondents answered that they received TSA's reports from other sources and 27 percent (18 of 97) of respondents answered that they received TSA's assessments from other sources.

[28] Aviation, highway, and rail survey respondents reported receiving transportation security-related information reports at a rate of 78 percent, 67 percent, and 84 percent respectively.

[29] Aviation, highway, and rail survey respondents reported receiving TSA assessments at a rate of 36 percent, 36 percent, and 41 percent respectively.

TSA uses different approaches to disseminate its security-related information products among the aviation, rail, and highway modes, which may help explain some of the variation in products received across modes. For example, TSA officials responsible for overseeing the freight rail sector said that they maintain contact information for each of their approximately 565 industry stakeholders and aim to provide TSA-OI products directly to the rail security coordinators designated by each railroad. In contrast, TSA officials responsible for overseeing the highway and motor carrier sector said that they share security-related information on a more selective basis because of the large number and broad nature of highway stakeholders. With tens of thousands of stakeholders—including bus, truck, and motor coach operators—across the country, it is not practical for TSA to reach every stakeholder. Therefore, TSA relies on communications with representatives from these industries rather than individual stakeholders.[30] According to TSA officials, TSA works with industry associations to distribute security-related information because leveraging these partnerships allows TSA to broaden its ability to reach stakeholders. However, stakeholders who are not affiliated with industry associations may not receive these communications. For example, according to the United Motorcoach Association, as many as two-thirds of companies in their sector were not represented by an industry association. While we recognize that not all stakeholders can receive every product, stakeholders included in our survey were identified by TSA as those who should be receiving this information.

Receiving a full range of TSA security-related information products could help stakeholders improve their situational awareness or change their operations to better protect their facilities and assets. For example, an official from a domestic passenger air carrier also told us that improved information sharing could have prevented their airline from diverting a plane with a disruptive passenger on board to Detroit, Michigan on the same day that a passenger attempted to detonate explosives aboard another Detroit-bound airplane on Christmas day 2009. This official told us that they had not been informed of this attempted bombing and stated

[30] The highway system included more than 4,000,000 miles of interstate and other roads, approximately 600,000 bridges, and more than 360 tunnels with more than 254 million registered vehicles as of 2007. As of 2008, the motor carrier industry was comprised of more than 29,000 motor coach buses, 475,000 school buses (as of 2009), and more than 26 million trucks (as of 2004).

that they would have diverted their company's plane elsewhere to prevent panic.

Most Stakeholders Who Used Information-sharing Mechanisms Were Generally Satisfied; Others Were Unfamiliar with DHS's Primary Mechanism

Aviation Stakeholders Were Generally Satisfied with TSA's Aviation Web Boards

The mechanisms used by TSA to share information with transportation stakeholders include the Aviation Web Boards, the Homeland Security Information Network (HSIN), and e-mail alerts. TSA's Aviation Web Boards serve as the principal information-sharing mechanism used to share information with the aviation mode, according to TSA officials.[31] Almost all (174 of 176) of the aviation stakeholders responded to our survey that they had heard of one of the Web Boards. Our survey results indicate that aviation stakeholders were generally satisfied with the Web Boards, with more than 70 percent of aviation respondents satisfied with

[31] The Aviation Web Boards were a mechanism used by the Federal Aviation Administration (FAA) prior to the creation of TSA, and were continued as a mechanism for aviation stakeholders after HSIN was established by DHS as the primary information-sharing mechanism for critical sectors. TSA's Commercial Aviation TSNM office stated that TSA uses the Web Boards in order to provide intelligence information at a single location while safeguarding Sensitive Security Information. Both TSA officials and aviation stakeholders we interviewed stated that the Web Boards might be viewed principally as a mechanism for disseminating regulatory information rather than threat-related information in some sectors.

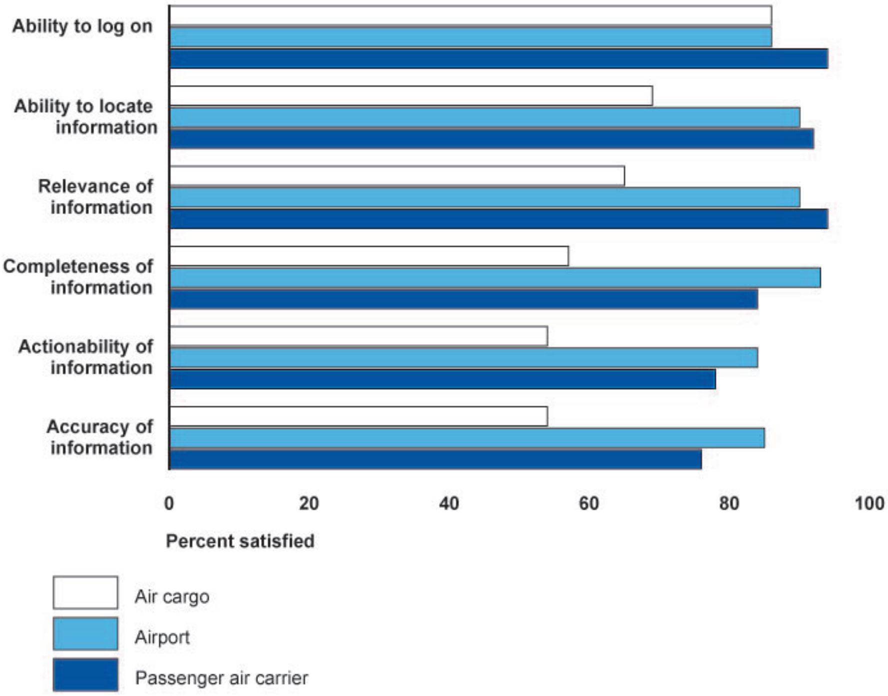
the ability to locate information, and the relevance, completeness, actionability, and accuracy of the information on the Web Boards.[32]

Compared to airports and passenger air carriers, air cargo stakeholders expressed lower levels of satisfaction with the Web Boards, as shown in figure 5. Specifically, less than 60 percent of air cargo stakeholders responding to the survey were satisfied with the accuracy, actionability, and completeness of information on the Web Boards.[33] Open-ended comments provided by air cargo stakeholders did not explain why they reported less satisfaction than other aviation sectors that have the same access to the Web Boards. Additionally, air cargo stakeholders provided open-ended comments that were similar to those of passenger air carriers and airport stakeholders. However, we observed that TSA has established individual Web Boards for each of the sectors, and not all aviation stakeholders have access to the same Web Boards.

[32] Specifically, 89 percent (154 of 174) of aviation stakeholders were very or somewhat satisfied with ability to log on; 84 percent (145 of 173) were very or somewhat satisfied with their ability to locate information; 84 percent (144 out of 172) were very or somewhat satisfied with relevance of information on Web Boards; 80 percent (136 of 171) were very or somewhat satisfied with completeness; 74 percent (125 of 170) were very or somewhat satisfied with actionability; and 73 percent (125 of 171) were satisfied with accuracy.

[33] Specifically, 54 percent (27 of 50) of air cargo stakeholders responding to the survey were very or somewhat satisfied with accuracy; 54 percent (27 of 50) were very or somewhat satisfied with actionability; and 57 percent (29 of 51) were very or somewhat satisfied with completeness of information on the Web Boards.

Figure 5: Percent of Satisfaction with Quality Indicators for TSA's Aviation Web Boards, by Aviation Sector



Source: GAO analysis of survey responses.

TSA and industry representatives provided some potential factors that may be affecting satisfaction among air cargo stakeholders. First, although TSA-OI officials stated that they are not sure why air cargo stakeholders are less satisfied, they noted that the Air Cargo TSNM office has not yet set up a direct interface between air cargo stakeholders and TSA-OI in which they could define their informational needs, as some other sectors have. Officials from the Air Cargo TSNM office did not indicate any plans to do so. Second, an industry association representing regional air cargo carriers stated that TSA does not seem to understand the information needs of the regional air cargo business, push out TSA-OI products to regional carriers, or conduct as much outreach to them as it does to major carriers.[34] While air cargo stakeholders expressed lower satisfaction than other aviation sectors, more than half stated that they were satisfied with all of the quality indicators covered in our survey related to the security-related information they receive from TSA. Officials from the Air Cargo TSNM office did not indicate any plans to change the way outreach is conducted to its air cargo stakeholders.

Although HSIN Is DHS's Primary Information-sharing Mechanism, Low Awareness and Less Satisfaction with Ability to Locate Information Hinder Its Use

Improving Outreach and Performance Measures Could Increase Awareness

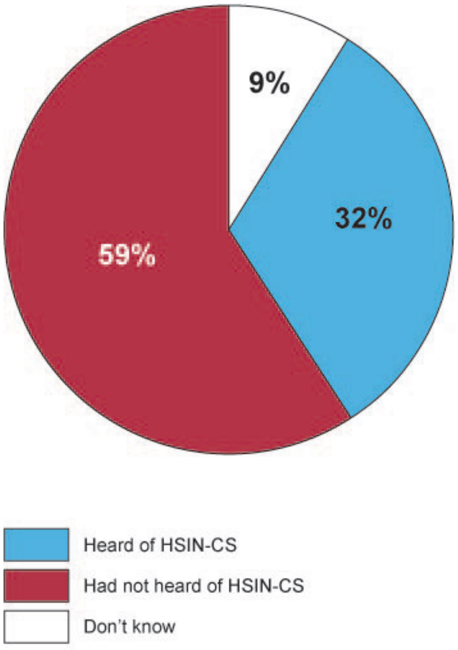
TSA aims to provide the right information to the right people at the right time through collaboration within and across the transportation sector network, according to TSA's TSISP. In addition, GAO's *Standards for Internal Control in the Federal Government* states that agencies should ensure adequate means of communicating with external stakeholders who may have a significant impact on agency goals and that effective information technology management is critical to achieving useful, reliable, and continuous communication of information.[35] HSIN is a national secure web-based portal—owned and maintained by DHS and other domestic and international users in a mission partnership with DHS—that was established for information sharing and collaboration between the federal, state, local, and private sectors engaged in the homeland security mission. DHS has stated that HSIN-CS is to be the

[34] Regional air cargo carriers include operators that transport cargo to regional airports in smaller communities, while major air cargo carriers utilize large jets that fly to major cities nationally and globally.

[35] In addition, according to the 2009 National Infrastructure Protection Plan (NIPP), efficient information sharing enables both government and private sector partners to assess events accurately, formulate risk assessments, and determine appropriate courses of action. A network approach enables secure, multidirectional information sharing between and across government and industry. This approach provides mechanisms, using information-protection protocols as required, to support the development and sharing of strategic and specific threat assessments, threat warnings, incident reports, all-hazards consequence reports, risk assessments, and best practices.

primary information-sharing mechanism for critical infrastructure sectors, including the transportation sector.[36] However, as shown in figure 6, almost 60 percent (158 of 266) of transportation stakeholders we surveyed had never heard of HSIN-CS.[37]

Figure 6: Percent of Stakeholders Who Had Heard of HSIN-CS



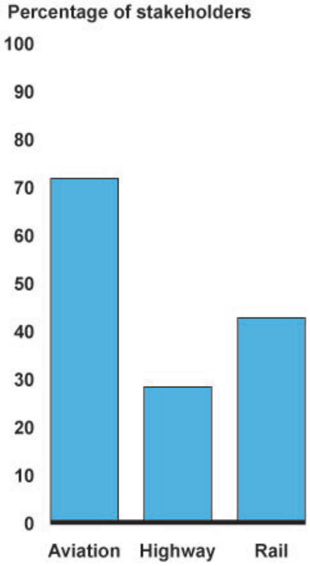
Source: GAO analysis of survey responses.

[36] Critical infrastructure includes the Defense Industrial Base; Energy; Food and Agriculture: Healthcare and Public Health; National Monuments and Icons; Banking and Finance; Water; Chemical; Commercial Facilities; Critical Manufacturing; Dams; Emergency Services; Nuclear Reactors, Materials, and Waste; Information Technology; Communications; Postal and Shipping; Transportation Systems (including aviation); and Government Facilities.

[37] Most of the survey recipients that had not heard of HSIN (78 percent) were aviation stakeholders, who utilize the Web Boards to access TSA information. Our survey population included more stakeholders from the aviation mode than the rail and highway modes.

Awareness and usage of HSIN-CS varied by transportation mode. As figure 7 shows, 72 percent of aviation stakeholders (124 of 173) responding to the survey had not heard of HSIN-CS and 9 percent (15 of 173) were unsure, and several commented that they would be interested in accessing the system. Among aviation stakeholders, the Web Boards were the more commonly utilized information-sharing mechanism. Among the highway respondents, 28 percent (11 of 39) had not heard of HSIN-CS and 8 percent (3 of 39) were unsure. Of the highway stakeholders who had heard of HSIN-CS, 60 percent (15 of 25) had a user account for the system and had accessed it. Less than half (25 of 54) of the rail respondents had heard of HSIN-CS and 11 percent (6 of 54) were unsure. Of the rail stakeholders who had heard of HSIN-CS, 64 percent (16 of 25) had a user account for the system and had accessed it.

Figure 7: Percentage of Stakeholders Who Had Not Heard of HSIN-CS by Mode



Source: GAO analysis of survey responses.

Similarly, in September 2010 we reported on a lack of awareness of the public transit subportal on HSIN (HSIN-PT) among public transit agencies we surveyed. We recommended that TSA establish time frames for a working group of federal and industry officials to consider targeted outreach efforts to increase awareness of HSIN-PT among transit agencies that are not currently using or aware of this system.[38] DHS officials concurred with this recommendation and in January 2011 provided an implementation plan with target dates for addressing it. However, the plan did not fully address the recommendation. For example, the plan stated that TSA officials created a consolidated “superlist” of current members of another information-sharing mechanism and invited them to join HSIN-PT. However, the plan did not indicate how TSA would target its outreach efforts to those entities not already on TSA’s lists. In a September 2011 update, TSA indicated that its working group would conduct outreach to smaller transit agencies but did not provide an estimated date for completing these actions.

Additional outreach by DHS and TSA to some transportation stakeholders could increase awareness of HSIN-CS. With its role in sharing security-related information with the private sector, the DHS National Protection and Programs Directorate’s Office of Infrastructure Protection has sector specialists and an outreach program to raise awareness of HSIN-CS, but, according to officials from this office, does little outreach to aviation stakeholders because committees that were intended to facilitate communication between the aviation industry and government have not been active.[39] DHS officials noted that there is a HSIN-CS portal for the aviation mode, but without input from the industry committees, DHS cannot develop it to meet the needs of aviation stakeholders. By contrast, facilitated communications with highway and motor carrier and rail stakeholders have resulted in the development of mode-specific HSIN-CS portals and improved outreach, according to DHS officials. For example, officials from the Freight Rail TSNM office stated that it tries to maintain

[38] GAO-10-895.

[39] These committees include the Sector Coordinating Councils (SCCs) and the Government Coordinating Councils (GCCs). The NIPP defines the organizational structures that provide the framework for coordination of critical infrastructure protection efforts at all levels of government, as well as within and across sectors. Sector-specific planning and coordination are addressed through coordinating councils that are established for each sector. SCCs comprise the representatives of owners and operators, generally from the private sector. GCCs comprise the representatives of the federal sector-specific agencies; other federal departments and agencies; and state, local, tribal, and territorial governments. These councils create a structure through which representative groups from all levels of government and the private sector can collaborate or share existing approaches to critical infrastructure protection and work together to advance capabilities.

direct contact with its more than 500 stakeholders in addition to reaching out to industry associations. The Highway and Motor Carrier TSNM office also uses industry associations to help communicate with various industries about HSIN-CS because its stakeholder group includes millions of people.[40] However, these outreach efforts do not reach stakeholders who fall outside of certain regions and are not members of an association.

TSA lacks outcome-oriented performance measures for HSIN-CS outreach and therefore cannot measure the effectiveness of its outreach and product dissemination. We have previously reported that leading management practices emphasize that successful performance measurement focuses on assessing the results of individual programs and activities.[41] We recognize and have previously reported on the challenge of assessing the effectiveness of security-related activities such as information sharing and developing outcome-oriented measures, but have called on agencies to take steps towards establishing such measures to hold them accountable for the investments they make. In September 2010, we reported that TSA had not developed specific performance goals or outcome-oriented measures for HSIN-PT, nor for TSA-OI's portal on HSIN-CS, now called TSA Intel on HSIN. TSA had developed an output-oriented performance measure for tracking the number of users of TSA Intel on HSIN; however, this measure provided limited information on which the agency could assess the results and progress of this information-sharing mechanism. We recommended that a working group establish time frames for developing goals and related outcome-oriented measures specific to TSA Intel on HSIN.[42] DHS concurred, noting that TSA would work with DHS and industry representatives to develop outcome-oriented metrics to assess the

[40] In contrast to the TSNM offices' interactions with rail and highway stakeholders, officials from the Commercial Aviation TSNM offices and Air Cargo TSNM office stated that they do not utilize HSIN-CS because they prefer the Aviation Web Boards.

[41]For example, see GAO, *Managing for Results: Enhancing Agency Use of Performance Information for Management Decision Making*, GAO-05-927 (Washington, D.C.: Sept. 9, 2005); *Program Evaluation: Studies Helped Agencies Measure or Explain Program Performance*, GAO/GGD-00-204 (Washington, D.C.: Sept. 29, 2000); *Managing for Results: Strengthening Regulatory Agencies' Performance Management Practices*, GAO/GGD-00-10 (Washington, D.C.: Oct. 28, 1999); and *Agency Performance Plans: Examples of Practices That Can Improve Usefulness to Decisionmakers*, GAO/GGD/AIMD-99-69 (Washington, D.C.: Feb. 26, 1999).

[42] This working group is specific to the public transit sector.

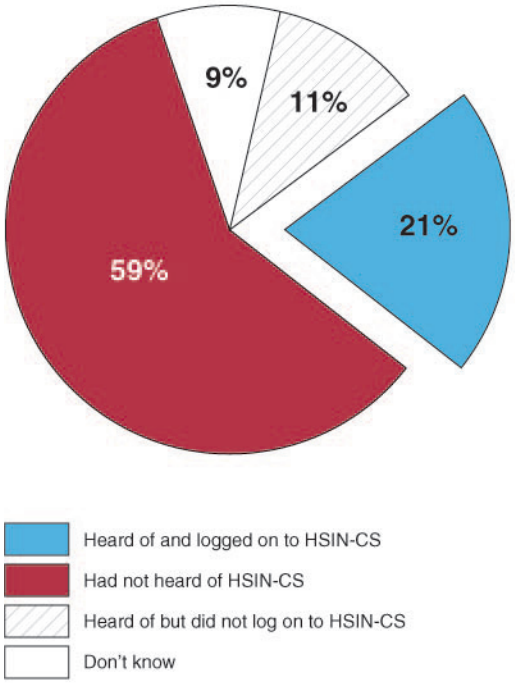
effectiveness of its information-sharing efforts. However, as of October 2011, TSA had not developed specific goals or outcome-oriented performance measures for TSA Intel on HSIN. TSA-OI officials stated that the only measure currently available to track dissemination is by counting "hits" on its intranet and internet portals, and told us that this method could be improved. The absence of measurable outcomes for targeted outreach to different transportation sectors hinders DHS efforts to ensure dissemination of security-related information to all appropriate stakeholders.[43] DHS's outreach efforts have not resulted in widespread HSIN-CS awareness and use among transportation stakeholders who we surveyed, and therefore conducting targeted outreach to stakeholders, and measuring the effectiveness of this outreach, could help to increase awareness and use of this mechanism.

Improving Search Function Could Increase User Satisfaction

With respect to stakeholder satisfaction with HSIN-CS, 21 percent of respondents (55 of 266) had logged on to HSIN-CS and could report whether they were satisfied with the mechanism, as shown in figure 8.

[43] TSA-OI officials told us in September 2010 that it would exclusively use its subportal on HSIN-CS to provide its security-related products to 100 percent of homeland security stakeholders. However, in a subsequent meeting in August 2011, TSA-OI officials said that they are considering a different approach in which they would use any mechanisms already in place and used by different stakeholder groups. However, until TSA demonstrates that the approach under consideration can be implemented, HSIN-CS remains the primary mechanism for providing security-related information to state, local, and private stakeholders seeking homeland security information.

Figure 8: Percent of Stakeholders that Had Heard of and Logged On To HSIN-CS



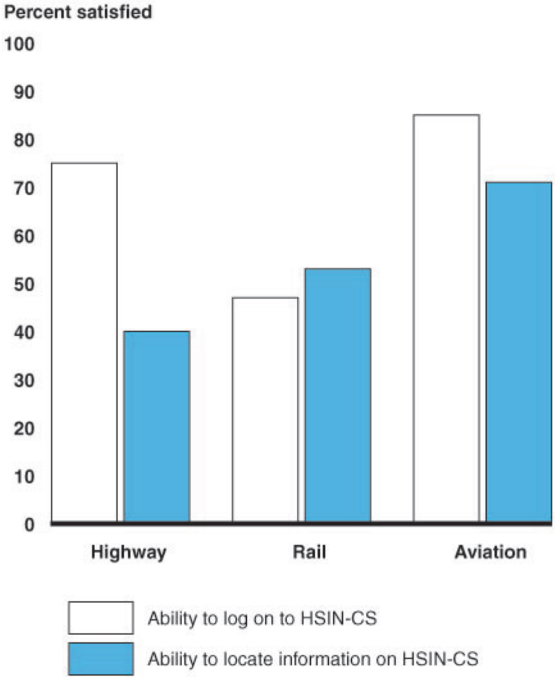
Source: GAO analysis of survey responses.

Survey results indicate that stakeholders who had logged on to HSIN-CS experienced difficulties in locating information on HSIN-CS.[44] Of those that logged on to HSIN-CS, 40 percent (6 of 15) of highway stakeholders and 53 percent (9 of 17) of rail stakeholders were satisfied with their ability to locate information on HSIN-CS, as shown in figure 9. A rail stakeholder who was less than satisfied noted in open-ended comments on the survey and in an interview that HSIN-CS was difficult to navigate with its many layers and that he could not find information for which he was searching. When we attempted in August 2011 to search for TSA security-related information products using the HSIN-CS search tool, we

[44] Similarly, the DHS Office of Inspector General found in June 2006 that state and local users of HSIN said that the search functionality was not reliable or effective in locating documents or information they needed to perform their work. See DHS OIG, *Homeland Security Information Network Could Support Information Sharing More Effectively*, OIG-06-38 (Washington, D.C.: June 2006).

encountered similar difficulties. For example, knowing that a Freight Rail Modal Threat Assessment released in March 2011 mentioned Toxic Inhalation Hazards, we searched HSIN-CS for this information using the search tool, sorting results by date, but could only find the Freight Rail Modal Threat Assessment from September 2009. Furthermore, when we restricted the search to the “rail/pipeline” sector, no information products appeared. Such difficulties may hinder HSIN-CS from meeting the security information needs of transportation stakeholders, and therefore limit TSA in its goal of achieving useful, reliable, and continuous communication of information. A TSA official agreed that the search function on HSIN-CS has technical limitations that can affect the user’s ability to locate information.

Figure 9: Percent of Stakeholders Satisfied with Usability of HSIN-CS by Mode

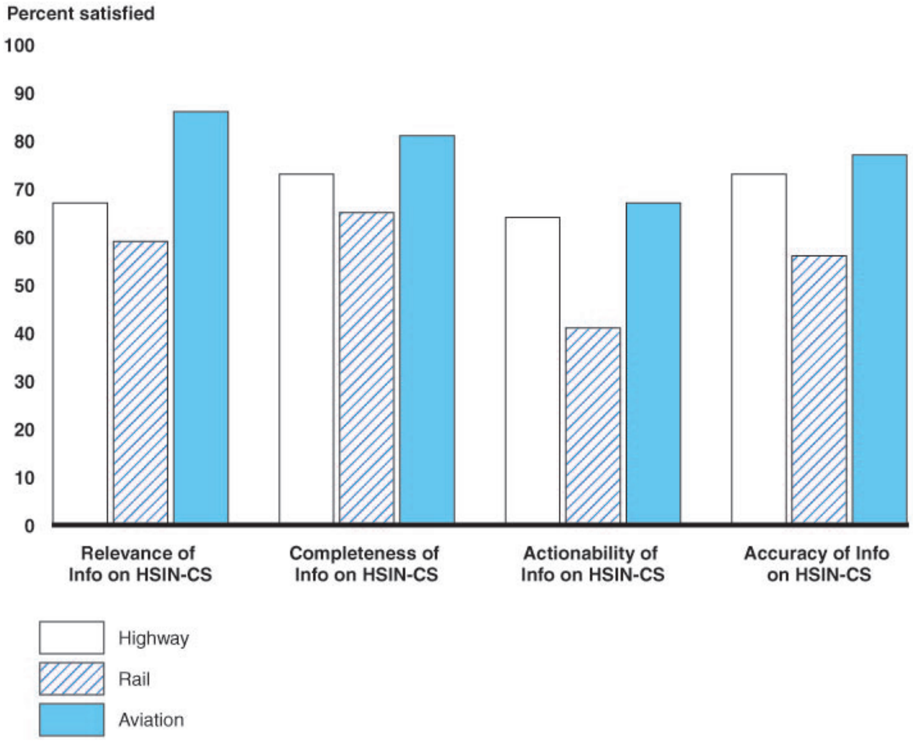


Source: GAO analysis of survey responses.

Note: 21 percent of survey recipients (55 of 266) had logged on to HSIN-CS and could therefore report on their satisfaction. Of these, 15 were highway stakeholders, 16 were rail stakeholders, and 24 were aviation stakeholders.

Stakeholder satisfaction with the quality of the information on HSIN-CS varied by mode, as shown in figure 10. For most aspects of HSIN-CS on which we surveyed stakeholder satisfaction (five of six), aviation stakeholders responding to the survey were the most satisfied, and rail stakeholders were the least satisfied.

Figure 10: Satisfaction with Quality of Information on HSIN-CS by Mode



Source: GAO analysis of survey responses.

Note: 21 percent of survey recipients (55 out of 266) had logged on to HSIN-CS and could therefore report on their satisfaction. Of these, 15 were highway stakeholders, 16 were rail stakeholders, and 24 were aviation stakeholders.

In September 2010, we reported that certain aspects of HSIN-PT were not user-friendly.[45] For example, 5 of 11 agencies that had access to HSIN-PT and used it to receive security-related information reported problems with using the system once they logged in. We recommended that DHS take steps to ensure that public transit agencies can access and readily utilize HSIN-PT and that HSIN-PT contain security-related information that is of value to public transit agencies. DHS concurred and

[45] GAO-10-895.

in January 2011 provided an implementation plan with target dates for addressing it. However, a September 2011 update to the plan did not include estimated dates for completing the actions. Further, the plan did not provide enough details about the actions to determine whether the agency is taking the necessary steps to address the recommendation.

Taking steps to ensure transportation stakeholders can access and readily use HSIN-CS—including improving the search function—could help DHS improve capacity of HSIN-CS to meet those stakeholders' security-related information needs. Because many transportation stakeholders have not heard of HSIN-CS, do not access the system, or encounter difficulties once they log in, they may not be receiving timely information via the information-sharing mechanism that DHS has established. DHS officials stated that our previous work has prompted ongoing efforts to address these concerns. However these efforts are primarily focused on working with public transit stakeholders to improve HSIN-CS for that mode. DHS officials stated that improvements to HSIN-CS and its portals for other modes is dependent on input and involvement from industry stakeholders.

E-mail Alerts Serve as Additional Information-sharing Mechanism, but Reach and Satisfaction Vary by Mode

TSA also described its e-mail alerts as a key information-sharing mechanism. Fifty-seven percent of survey respondents (149 of 263 who answered the question) reported receiving a TSA e-mail alert. Sixty-nine percent (37 of 54) of rail stakeholders received e-mail alerts, compared with 58 percent (100 of 173) of aviation stakeholders, and 33 percent (12 of 36) of highway stakeholders.

Overall, more than half of stakeholders were satisfied with the five dimensions of quality, ranging from 74 percent (115 of 154) of respondents satisfied with relevance to 64 percent (96 of 151) of respondents satisfied with the accuracy of the e-mail alerts. In general, of those that received an e-mail alert, highway stakeholders were the most satisfied and rail stakeholders were the least satisfied. It is not clear why stakeholders from different modes reported different levels of satisfaction, and stakeholders did not offer open-ended comments explaining their satisfaction levels.

Defining and Documenting Roles and Responsibilities within TSA Could Help Strengthen Information Sharing

The approach that TSA uses to communicate security-related information to stakeholders relies on partnerships established among offices within the agency. A good internal control environment requires that the agency's organizational structure clearly define key areas of authority and responsibility and establish appropriate lines of reporting.[46] We have previously reported that collaborating agencies should work together to define and agree on their respective roles and responsibilities. In doing so, agencies can clarify who will do what, organize their joint and individual efforts, and facilitate decision making.[47] TSA-OI officials told us that the TSNM offices for each transportation mode serve as the primary contact to stakeholders. However, the specific roles and responsibilities of each office in sharing security-related information with stakeholders are not clearly defined. While TSA-OI depends on the TSNM offices to provide security-related information directly to stakeholders in individual transportation modes, officials from TSA-OI also stated that the responsibility for disseminating transportation security information to intended targets is shared with TSA-OI. However, because of the different dynamics of each transportation mode, TSA-OI defers to the individual modal TSNM offices in deciding how to help industry stakeholders obtain TSA-OI information.

TSA officials from five TSNM offices provided different interpretations of the Office of TSNM's roles and responsibilities in disseminating TSA-OI products and other security-related information. Officials from three of these offices stated that the TSNM offices are the primary means for disseminating security-related information products, with two of the three stating that part of this responsibility is informing stakeholders of TSA's Intel page on HSIN-CS. However, officials from two other TSNM offices stated that the role of the TSNM offices is limited to communicating policy and regulatory information rather than threat-related information. Additionally, stakeholders differed among and within modes in the extent to which they would contact the TSNM office to obtain security-related information. For example, one aviation stakeholder stated that it would call the TSNM office directly if it needed a product or information while

[46] GAO, *Internal Control, Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999).

[47] GAO, *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, GAO-06-15 (Washington, D.C.: Oct. 21, 2005).

another stated that they would contact their Federal Security Director at the local airport for the same information.

Our survey results indicate that some stakeholders are not receiving TSA's security-related information products and others are not aware of the mechanisms available to them. While officials from both TSA-OI and the Office of TSNM told us that the responsibility for ensuring that stakeholders are receiving security-related products lies within their offices, the roles and responsibilities are not documented and are open to interpretation. TSA officials told us that they do not currently have an information flow diagram or document describing or mandating information sharing between TSA-OI and the Office of TSNM because the two offices share information on a daily basis and discuss routing to internal and external stakeholders. Further, TSA officials stated that information flow regarding transportation security is dynamic and complex with varying levels of classification, audiences, and topics. While it is recognized that information products and mechanisms are selected and utilized as appropriate to the circumstances, clearly documenting the basic roles and responsibilities of its partners—especially TSNM offices—in sharing security-related information with transportation stakeholders and increasing awareness of information-sharing mechanisms could improve the effectiveness of TSA-OI's information-sharing efforts and help ensure accountability.

Additionally, key elements of TSA's information approach are not described in its December 2010 information-sharing plan. The 9/11 Commission Act requires DHS to annually submit an information-sharing plan to Congress that describes how intelligence analysts within the department will coordinate their activities within the department and with other federal, state, and local agencies, and tribal governments, among other things.[48] TSA is the lead agency in developing the TSISP and describes the plan as an annual report that establishes a foundation for sharing transportation security information between all entities that have a stake in protecting the nation's transportation system. TSA is not required to share the plan with stakeholders but coordinates its updates with input from the mode-specific SCCs. TSA officials described the plan as overarching guidance for information-sharing activities within TSA.

[48] Pub. L. No. 110-53, § 1203(a), 121 Stat. 266, 383-85 (2007) (codified at 49 U.S.C. § 114(u)(6)). TSA has replaced the ISAC with TSA's Intel page on HSIN.

Additionally, the Transportation Systems Sector Specific Plan describes the TSISP as including the process for sharing critical intelligence and information throughout the sector.[49] It states that the TSISP reflects a vertical and horizontal network of communications for timely distribution of accurate and pertinent information. The last update to the plan was December 2010. However, this plan does not describe key information-sharing functions and programs, as follows:

- The TSISP does not acknowledge that the Aviation Web Boards are the primary mechanism used for sharing security-related information with the aviation community. TSA officials stated that this is the primary tool used to share information with commercial aviation airports and passenger air carriers as well as air cargo carriers. Aviation stakeholders we interviewed confirmed that the Web Boards are their primary means of receiving information from TSA. TSA officials stated that a description of the Aviation Web Boards was intentionally removed from a draft of the plan at the request of the Commercial Aviation TSNM office. They did not offer an explanation for why the description was removed.
- The Field Intelligence Officer (FIO) program is expanding and is an integral part of TSA's information-sharing environment. However, roles and responsibilities of FIOs are not described in detail in the 2010 TSISP. According to TSA, the FIOs serve as the principal advisor to Federal Security Directors and their staffs on all intelligence matters. Other responsibilities include developing and maintaining a working relationship with local, federal, state, and private entities responsible for transportation security, regardless of mode. While officers are based at the airports, they interact with the security officials from local rail, mass transit, highway, and port and pipeline (where applicable) modes to facilitate the sharing and exchange of relevant threat information. As of August 2011, approximately 40 FIOs were deployed, with a goal of 66 FIOs by the end of 2012.

TSA-OI stated that it has several planned changes to its information-sharing strategy but has not yet issued them in a documented plan that identifies the specific roles and responsibilities of its internal partners,

[49] The Transportation Systems Sector Specific Plan describes collaboratively developed strategies to reduce risks to critical transportation infrastructure from the broad range of known and unknown terrorism threats. DHS, *Transportation Systems Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan (*Washington, D.C.: 2010).

specific goals for information sharing, and how progress in meeting those goals is measured.

Conclusions

Securing the nation's vast and diverse transportation system is a challenging task that is complicated by the ever-changing and dynamic threat environment. As new threats emerge and vulnerabilities are identified, dissemination of timely and actionable information is critical to maintaining the security of our nation. While providing federal, state, local, tribal, and private sector partners with the information they need can be complicated, providing them with the right information at the right time can prevent catastrophic losses from terrorist activities targeted at the transportation modes. However, stakeholders cannot act on information that they do not receive or cannot access. At the same time, if the information stakeholders receive is not actionable, it is less valuable in helping them prioritize, manage, or adjust security operations. While specific actionable intelligence is not always available, providing these stakeholders with more actionable analysis would help allow them to adjust security measures or take other necessary actions to improve their security postures and counter past and present threats.

While TSA has taken steps to ensure that security-related information is available to stakeholders when they need it through various mechanisms, additional actions could help to ensure that stakeholders are aware of these resources and can access them when needed. Given that DHS's current outreach efforts have not resulted in widespread HSIN-CS awareness and use among transportation stakeholders, additional actions to improve system awareness and accessibility will help ensure that transportation security information users receive timely and useful security information. Additionally, developing outcome-oriented performance measures could help assess progress in improving the dissemination of key transportation security information to all appropriate stakeholders. Because TSA has not clearly defined and documented roles and responsibilities for disseminating security-related information and the full range of its information-sharing efforts, TSA may not be consistently providing security-related information products to external stakeholders and divisions within TSA may not be held fully accountable for performing their information-sharing activities. Clarifying the roles and responsibilities of TSA's various offices in sharing security-related information with transportation stakeholders could improve the effectiveness of TSA's information-sharing efforts and help ensure greater accountability.

Recommendations for Executive Action

To help strengthen information sharing with transportation stakeholders and ensure that stakeholders receive security-related information in a timely manner, we recommend that the Secretary of Homeland Security direct the Assistant Secretary for the Transportation Security Administration to take the following five actions:

- To the extent possible, address the need expressed by stakeholders by providing more actionable analysis in TSA's transportation security-related information products.
- In coordination with other DHS components, conduct targeted outreach efforts to aviation, rail, and highway stakeholders to increase the number of transportation stakeholders who are receiving security-related information products and are made aware of security information available through the HSIN-CS portal.
- Coordinate with other DHS components to improve the ability to readily locate information in TSA security-related information products on HSIN-CS.
- Establish outcome-oriented performance measures to help assess the results of efforts to provide useful and timely transportation security information through the HSIN-CS portal.
- Clearly define and document the specific information-sharing programs, activities, roles, and responsibilities for each TSA division and provide this information to the appropriate stakeholder groups.

Agency Comments and Our Evaluation

We provided a draft of this report and a draft copy of the accompanying e-supplement (GAO-12-67SP) to Amtrak and the Departments of Homeland Security and Transportation for comment. Amtrak did not provide written comments to include in our report. However, in an e-mail received October 28, 2011, the Amtrak audit liaison stated that Amtrak concurred with our recommendation concerning the need for TSA to provide more actionable analysis in its transportation security-related information products. DHS provided written comments on the draft report, which are reproduced in full in appendix II. DHS concurred with the findings and recommendations in the report and described the efforts the department has underway or planned to address our recommendations, as summarized below. The Department of Transportation's Deputy Director of Audit Relations replied in an e-mail received on October 27, 2011, that the department had no comments on the report. Amtrak and the Departments of Homeland Security and Transportation did not provide comments on the e-supplement.

In his e-mail, the Amtrak audit liaison noted that Amtrak recognizes the pressure that TSA is under to produce meaningful intelligence and information analysis to a diverse transportation industry where the information flow is dynamic and complex. However, Amtrak added that at the stakeholder level, the ability to quickly react and deploy to interdict a terrorist threat, planning cycle, or incident based upon information that is timely and actionable is crucial. According to Amtrak, improvements in this area could significantly improve private industry's ability to plan, defend, deter, and detect terrorist activities. Amtrak views its relationship with TSA as a very important and critical one in addressing Amtrak's security posture on a daily basis across the intercity rail system. Amtrak also noted that it maintains relationships with other federal, state, and international agencies to improve its intelligence and information-sharing capacity. According to Amtrak, the combination of all these resources allows Amtrak to stay abreast of intelligence trends and developing information and to sift quickly through data and look for rail-centric information.

In its written comments, DHS stated that, since the conclusion of our review, many of TSA's products now include analysis of threat levels, trends, tactics, techniques, and procedures. Since this new development occurred after our review, we did not evaluate the products referred to in the statement. We encourage TSA to continue these efforts and to work with stakeholder groups to ensure that the additional analysis and actionable information provided in these products meets their needs. DHS also stated that TSA will continue working with the DHS Office of Infrastructure Protection to help modal stakeholders understand the security information currently available on HSIN-CS and other systems. DHS provided several examples of other information sources it is using. While these may be appropriate systems for disseminating information to members of the intelligence or law enforcement communities, 272 of the 275 transportation stakeholders responding to our survey did not list any of these systems among their sources for security-related information. DHS stated that its strategy has evolved to consider stakeholders' preferred methods of receiving security-related information. However, it notes that this change has taken place since the conclusion of our review. As such, we are not able to evaluate this statement. We encourage TSA to increase its outreach efforts to ensure that stakeholders are aware of these mechanisms and information and take further steps to ensure that stakeholders are receiving TSA's information products through these sources. In addition, DHS stated that TSA plans to enhance the marketing of its information solutions, including HSIN-CS, and to align its partners with its information-sharing roles and responsibilities. While these are positive steps in encouraging information sharing with stakeholders, they do not address the concern stakeholders expressed regarding their ability to locate specific information on HSIN-CS. We continue to believe that improving the search function could enhance stakeholders' use of HSIN-CS in locating TSA products. Further, DHS said that TSA has started to develop a system to measure and monitor how stakeholders receive information, frequency of use, and methods used for customer outreach and obtaining customer feedback. Finally, DHS said that TSA will commit to creating an internal document of the roles and responsibilities of TSNM and TSA-OI for information sharing and share this document with the appropriate stakeholder groups. Doing so could help clarify responsibilities and increase accountability.

DHS also provided three technical clarifications in its written comments. First, DHS stated that TSA has already begun using multiple information systems to disseminate intelligence to stakeholders, and provided examples of these systems. However, as noted above, the examples provided were not identified as sources of information by 272 of the 275 transportation stakeholders who completed our survey. In addition, DHS stated that TSA's 2011 update to the TSISP is undergoing internal review and will reflect its enhanced information-sharing strategy and changes made as a result of our review, such as describing the information-sharing roles and functions of its Field Intelligence Officers. Finally, TSA stated the context concerning our discussion of the roles and responsibilities of TSA offices regarding the sharing of specific information such as intelligence was unclear. As stated in this report, we interviewed officials from TSA-OI and the Commercial Airline, Commercial Airport, Air Cargo, Freight Rail, and Highway and Motor Carrier units within TSNM on the functions they perform in information sharing. We also stated that TSA officials from five TSNM offices provided different interpretations of the Office of TSNM's roles and responsibilities in disseminating TSA-OI products and other security-related information. TSA noted in its letter that there are branches of the TSNM that do not interact with stakeholders. The statements in our report were based on discussions with officials from the TSNM modal offices that interact with stakeholders.

We are sending copies of this report to the Secretaries of Homeland Security and Transportation, and the President and Chief Executive Officer of Amtrak. The report is also available at no charge on GAO's website at http://www.gao.gov. Please contact me at (202) 512-4379 or lords@gao.gov if you have any questions regarding this report. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are acknowledged in appendix III.

Stephen Lord

Stephen M. Lord
Director, Homeland Security and Justice Issues

List of Committees

The Honorable Tim Johnson
Chairman
The Honorable Richard C. Shelby
Ranking Member
Committee on Banking, Housing, and Urban Affairs
United States Senate

The Honorable John D. Rockefeller IV
Chairman
The Honorable Kay Bailey Hutchison
Ranking Member
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable Joseph I. Lieberman
Chairman
The Honorable Susan M. Collins
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Peter T. King
Chairman
The Honorable Bennie G. Thompson
Ranking Member
Committee on Homeland Security
House of Representatives

The Honorable John L. Mica
Chairman
The Honorable Nick J. Rahall, II
Ranking Member
Committee on Transportation and Infrastructure
House of Representatives

Appendix I: Scope and Methodology

This report addresses the following questions: (1) To what extent are transportation stakeholders satisfied with the quality of the Transportation Security Administration's (TSA) transportation security-related information products? (2) To what extent are stakeholders satisfied with the mechanisms used to disseminate these products? (3) To what extent has TSA defined its roles and responsibilities for sharing security-related information with stakeholders?

To assess the extent to which stakeholders are satisfied with the security-related information products that they receive from TSA and the mechanisms used to obtain them, we conducted a web-based survey of transportation stakeholders from the aviation, freight and passenger rail, and highway modes.[1]

To develop the survey and to identify the primary security-related information-sharing products, mechanisms, and the stakeholders for whom TSA maintains contact information, we interviewed officials from TSA's Office of Intelligence (TSA-OI) and officials from the Commercial Airline, Commercial Airport, Air Cargo, Freight Rail, and Highway and Motor Carrier Transportation Sector Network Management (TSNM) offices.[2] We also interviewed officials from industry associations representing air carriers, airports, air cargo carriers, freight and passenger rail, short line and regional railroads, state highway transportation officials, bus, truck, and motor coach operators, and airport law enforcement. While the information provided by industry association officials is not generalizable to all industry stakeholders, these associations provided industry perspectives on broad security issues facing their respective stakeholder groups.

We designed draft questionnaires in close collaboration with GAO survey specialists. We conducted pretests with seven security officials—at least one from each of the sectors we surveyed—in person and by telephone. We also obtained input on a draft questionnaire from industry associations.

[1] GAO conducted a similar review on the satisfaction of public transit stakeholders in 2010 and therefore did not assess the satisfaction of public transit stakeholders in this review. See GAO-10-895.

[2] In September 2011, TSA announced that, as part of a headquarters realignment, TSA-OI will become part of a new Office of Intelligence and Analysis and the Office of TSNM will transition to the Office of Security Policy and Industry Engagement.

We identified organizations and security officials at each organization to receive the survey using TSA's security information product distribution lists and through interviews with aviation, passenger and freight rail, and highway industry organizations. We sent the survey to one security official at each of the organizations that we identified in our preliminary steps, which included commercial passenger air carriers, Category X and I commercial airports, air cargo carriers, Amtrak, Class I freight rail carriers, short line and regional railroads that carry toxic inhalation hazards or operate in high-threat urban areas, and state departments of transportation or emergency management.[3] We sent the survey to the entire known population of organizations; no sampling was conducted. Each official was asked to respond on behalf of the entire organization and to consult with other officials or records if necessary to do so.

We notified 339 officials on March 28, 2011, by e-mail that the survey was about to begin and updated contact information as needed. (We also learned at that time that 4 organizations had gone out of business or been consolidated, leaving 335 organizations as the total known population.) We launched our web-based survey on April 4, 2011, and asked for responses to be submitted by April 8, 2011. Log-in information was e-mailed to all contacts. We contacted by telephone and e-mailed those who had not completed the questionnaire at multiple points during the data collection period, and we closed the survey on May 18, 2011. A total of 275 organizations submitted a completed questionnaire with usable responses for an overall response rate of 82 percent, as shown in table 3.

[3] Category X airports represent the nation's largest and busiest airports as measured by the volume of passenger traffic and are potentially attractive targets for criminal and terrorist activity. TSA classifies the nation's airports into one of five categories (X, I, II, III, and IV) based on various factors such as the number of takeoffs and landings annually, the extent of passenger screening at the airport, and other security considerations. In general, Category X airports have the largest number of passenger boardings and Category IV airports have the smallest. As defined by revenue, for 2009, Class I railroads are freight rail carriers having an operating revenue of $379 million or more. Our survey responses represent each of the stakeholder groups described but are not generalizable to entire modes of transportation such as aviation, rail, and highways.

Table 3: Stakeholder Groups That Received and Completed the Survey

Stakeholder transportation sector and mode	Number that received the survey	Number that completed the survey	Percent of recipients that completed the survey
Aviation	**215**	**178**	**83**
Commercial passenger air carrier	61	50	82
Air cargo	71	53	75
Commercial airports	83	75	90
Rail	**68**	**58**	**85**
Class I freight rail	7	7	100
Shortline and regional freight rail	60	50	83
Amtrak	1	1	100
Highway	**52**	**39**	**75**
Total	**335**	**275**	**82**

Source: GAO survey.

The final instrument, reproduced in an e-supplement we are issuing concurrent with this report—GAO-12-67SP—displays the counts of responses received for each question.[4] The questionnaire asked those transportation stakeholders responsible for security operations to identify the modes of transportation they provide, the extent to which they receive and are satisfied or dissatisfied with TSA security-related products and briefings, the mechanisms they use to obtain security information, and their satisfaction with each of these mechanisms.

For the purposes of this survey, we defined the five aspects of security-related information quality as:

- timeliness: the degree to which you received the information within the time it was needed;
- relevance: the degree to which the information was applicable to your organization;
- completeness: the degree to which the information contained all the necessary details;

[4] GAO-12-67SP.

- actionability: the degree to which the information enabled you to make adjustments to your security measures, if such a change was warranted; and
- accuracy: the degree to which the information was correct.

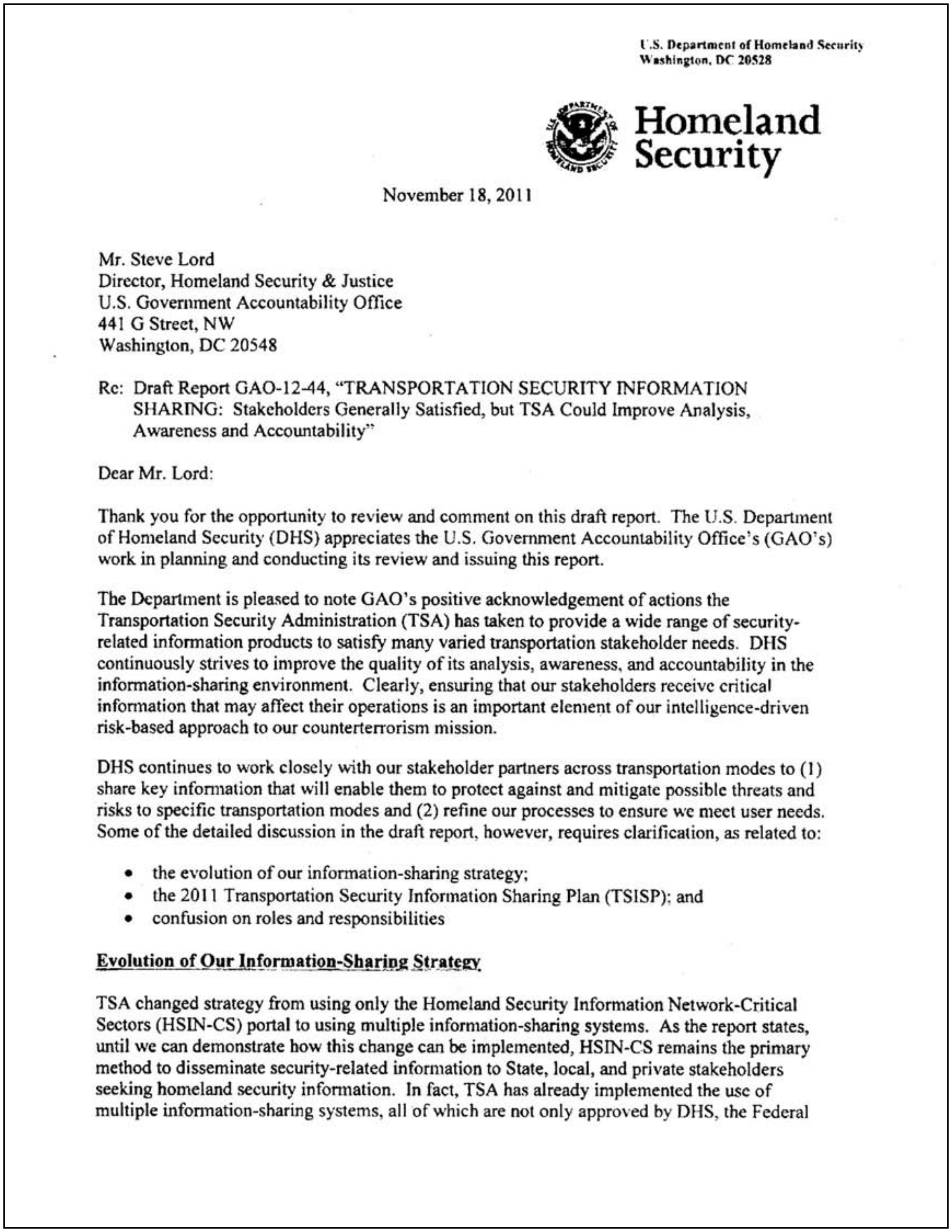
While all known organizations were selected for our survey, and therefore our data are not subject to sampling errors, the practical difficulties of conducting any survey may introduce nonsampling errors. For example, differences in how a particular question is interpreted, the sources of information available to respondents, or the types of people who do not respond to a question can introduce errors into the survey results. We included steps in both the data collection and data analysis stages to minimize such nonsampling errors. As we previously indicated, we collaborated with our survey specialists to design draft questionnaires, and versions of the questionnaire were pretested with seven members of the surveyed population. In addition, we provided a draft of the questionnaire to industry organizations for their review. From these pretests and reviews, we made revisions as necessary to reduce the likelihood of nonresponse and reporting errors on our questions. Our analysts answered respondent questions and resolved difficulties that respondents had in answering our questions. We examined the survey results and performed computer analyses to identify inconsistencies and other indications of error and addressed such issues, where possible. A second, independent analyst checked the accuracy of all computer analyses to minimize the likelihood of errors in data processing. To obtain additional narrative and supporting context from stakeholders, survey respondents were given multiple opportunities to provide additional open-ended comments throughout our survey. While the survey responses cannot be used to generalize the opinions and satisfaction of transportation stakeholders as a whole, the responses provide data for our defined population.

We also conducted site visits, or held teleconferences, with security and management officials from a nonprobability sample of 18 aviation, rail, and highway transportation stakeholders across the nation to determine specific areas of satisfaction and dissatisfaction with TSA security-related information products and which mechanisms are most routinely used by these stakeholders to obtain security-related information. These stakeholders were selected to generally reflect the variety of public and private entities in terms of size, location, and transportation mode. Because we selected a nonprobability sample of transportation stakeholders to interview, the information obtained cannot be generalized to the overall population of stakeholders. However, the interviews provided illustrative examples of the perspectives of various stakeholders about TSA's information-sharing products and mechanisms and corroborated information we gathered through other means.

To determine the extent to which TSA has defined and documented information-sharing roles and responsibilities, we reviewed documents, when available, that described TSA's information-sharing functions. Primarily, we reviewed the 2009 and 2010 Transportation Security Information Sharing Plans (TSISP). We compared the TSISPs to national plans and documents that describe recommended practices for information sharing such as the Information Sharing Council's Information Sharing Environment Implementation Plan and the National Infrastructure Protection Plan. We also reviewed our own standards for internal controls. Because TSA does not have an information flow diagram or document describing or mandating information sharing between TSA-OI and the TSNM offices, we interviewed senior TSA officials from TSA-OI and each of the modal TSNM offices to discuss their roles and responsibilities in sharing information with public and private stakeholders. We compared the officials' interpretations of their roles and responsibilities to identify the extent to which they were consistent across modes and offices.

We conducted this performance audit from May 2010 through November 2011 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 II: Comments from the Department of Homeland Security



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

Homeland
Security

November 18, 2011

Mr. Steve Lord
Director, Homeland Security & Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Draft Report GAO-12-44, "TRANSPORTATION SECURITY INFORMATION SHARING: Stakeholders Generally Satisfied, but TSA Could Improve Analysis, Awareness and Accountability"

Dear Mr. Lord:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO's) work in planning and conducting its review and issuing this report.

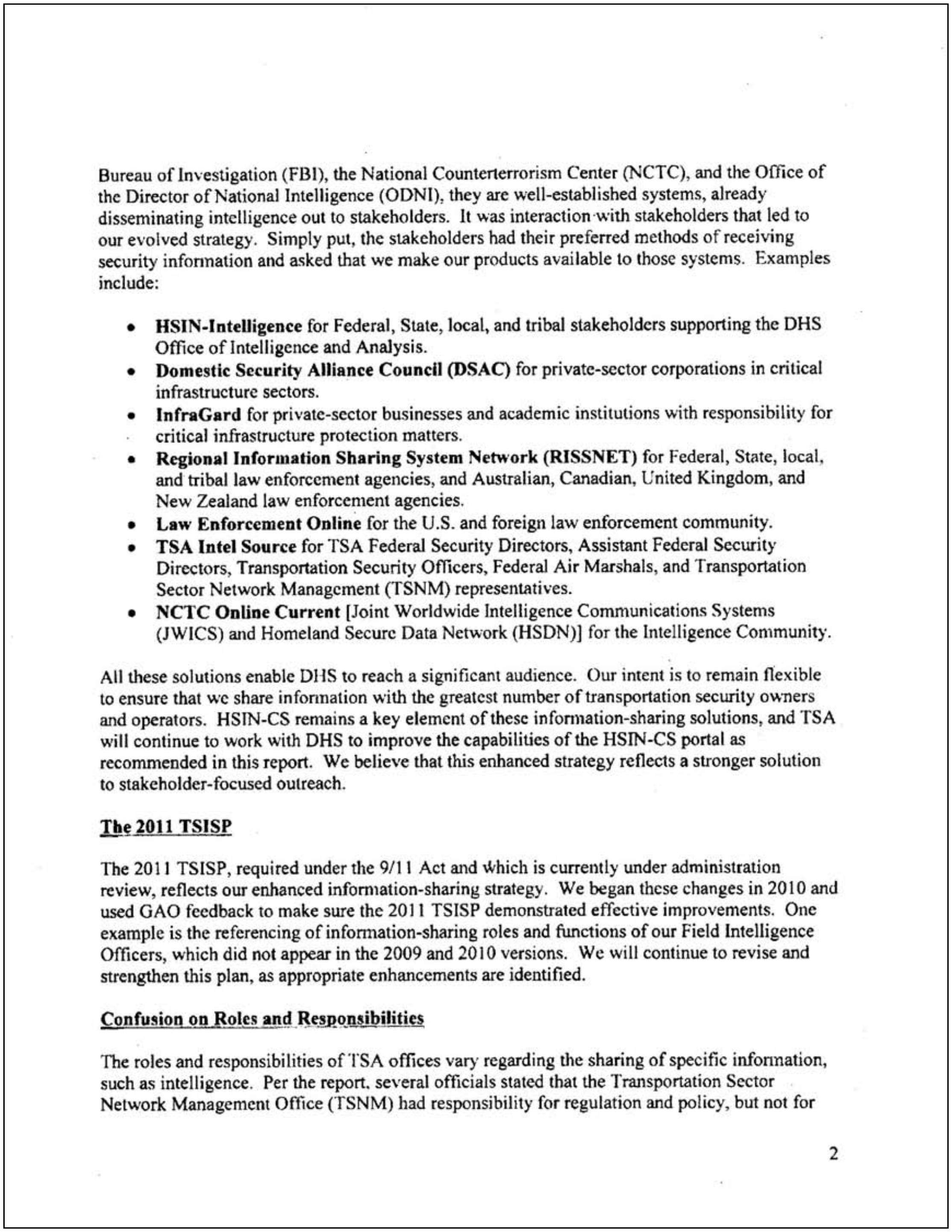
The Department is pleased to note GAO's positive acknowledgement of actions the Transportation Security Administration (TSA) has taken to provide a wide range of security-related information products to satisfy many varied transportation stakeholder needs. DHS continuously strives to improve the quality of its analysis, awareness, and accountability in the information-sharing environment. Clearly, ensuring that our stakeholders receive critical information that may affect their operations is an important element of our intelligence-driven risk-based approach to our counterterrorism mission.

DHS continues to work closely with our stakeholder partners across transportation modes to (1) share key information that will enable them to protect against and mitigate possible threats and risks to specific transportation modes and (2) refine our processes to ensure we meet user needs. Some of the detailed discussion in the draft report, however, requires clarification, as related to:

- the evolution of our information-sharing strategy;
- the 2011 Transportation Security Information Sharing Plan (TSISP); and
- confusion on roles and responsibilities

Evolution of Our Information-Sharing Strategy

TSA changed strategy from using only the Homeland Security Information Network-Critical Sectors (HSIN-CS) portal to using multiple information-sharing systems. As the report states, until we can demonstrate how this change can be implemented, HSIN-CS remains the primary method to disseminate security-related information to State, local, and private stakeholders seeking homeland security information. In fact, TSA has already implemented the use of multiple information-sharing systems, all of which are not only approved by DHS, the Federal



Bureau of Investigation (FBI), the National Counterterrorism Center (NCTC), and the Office of the Director of National Intelligence (ODNI), they are well-established systems, already disseminating intelligence out to stakeholders. It was interaction with stakeholders that led to our evolved strategy. Simply put, the stakeholders had their preferred methods of receiving security information and asked that we make our products available to those systems. Examples include:

- **HSIN-Intelligence** for Federal, State, local, and tribal stakeholders supporting the DHS Office of Intelligence and Analysis.
- **Domestic Security Alliance Council (DSAC)** for private-sector corporations in critical infrastructure sectors.
- **InfraGard** for private-sector businesses and academic institutions with responsibility for critical infrastructure protection matters.
- **Regional Information Sharing System Network (RISSNET)** for Federal, State, local, and tribal law enforcement agencies, and Australian, Canadian, United Kingdom, and New Zealand law enforcement agencies.
- **Law Enforcement Online** for the U.S. and foreign law enforcement community.
- **TSA Intel Source** for TSA Federal Security Directors, Assistant Federal Security Directors, Transportation Security Officers, Federal Air Marshals, and Transportation Sector Network Management (TSNM) representatives.
- **NCTC Online Current** [Joint Worldwide Intelligence Communications Systems (JWICS) and Homeland Secure Data Network (HSDN)] for the Intelligence Community.

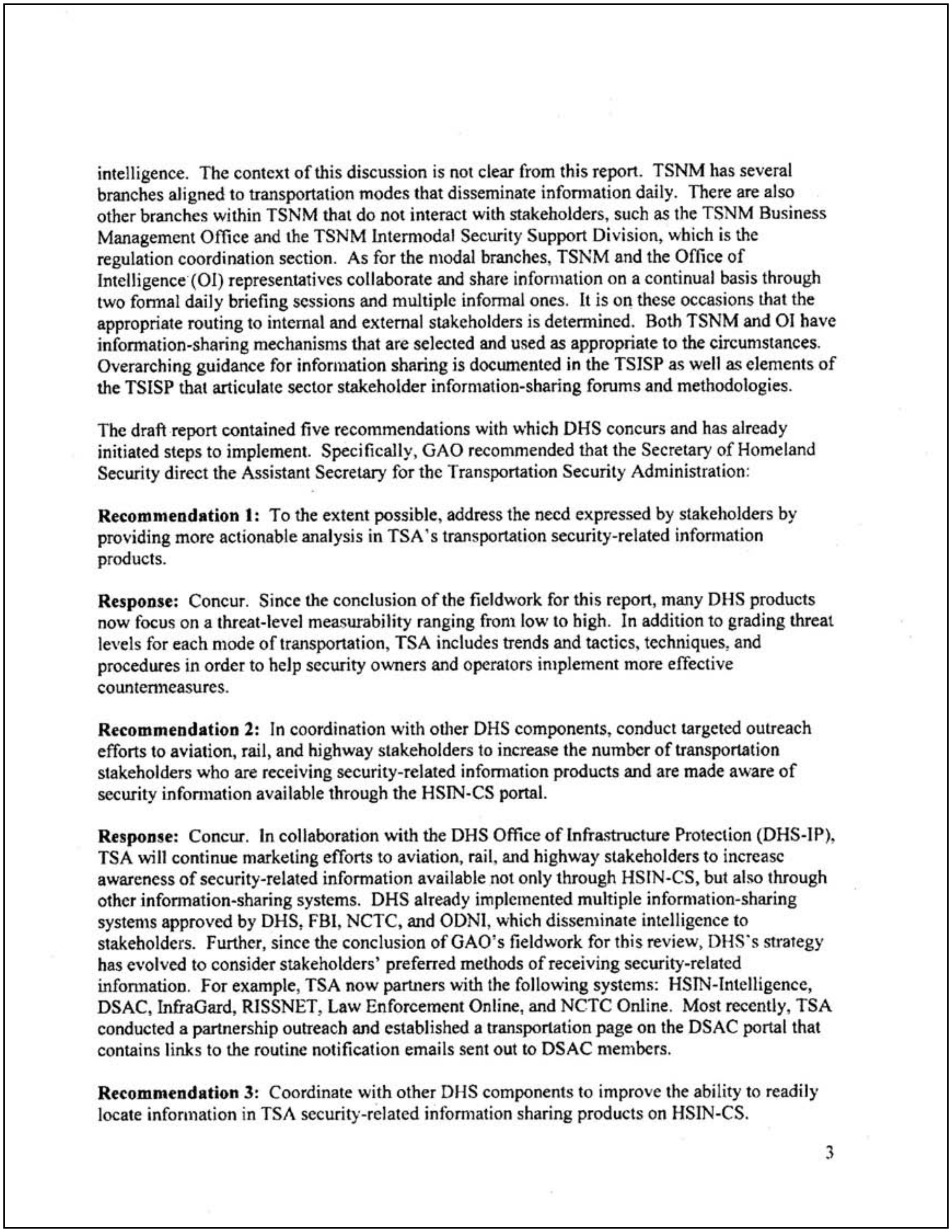
All these solutions enable DHS to reach a significant audience. Our intent is to remain flexible to ensure that we share information with the greatest number of transportation security owners and operators. HSIN-CS remains a key element of these information-sharing solutions, and TSA will continue to work with DHS to improve the capabilities of the HSIN-CS portal as recommended in this report. We believe that this enhanced strategy reflects a stronger solution to stakeholder-focused outreach.

The 2011 TSISP

The 2011 TSISP, required under the 9/11 Act and which is currently under administration review, reflects our enhanced information-sharing strategy. We began these changes in 2010 and used GAO feedback to make sure the 2011 TSISP demonstrated effective improvements. One example is the referencing of information-sharing roles and functions of our Field Intelligence Officers, which did not appear in the 2009 and 2010 versions. We will continue to revise and strengthen this plan, as appropriate enhancements are identified.

Confusion on Roles and Responsibilities

The roles and responsibilities of TSA offices vary regarding the sharing of specific information, such as intelligence. Per the report, several officials stated that the Transportation Sector Network Management Office (TSNM) had responsibility for regulation and policy, but not for



intelligence. The context of this discussion is not clear from this report. TSNM has several branches aligned to transportation modes that disseminate information daily. There are also other branches within TSNM that do not interact with stakeholders, such as the TSNM Business Management Office and the TSNM Intermodal Security Support Division, which is the regulation coordination section. As for the modal branches, TSNM and the Office of Intelligence (OI) representatives collaborate and share information on a continual basis through two formal daily briefing sessions and multiple informal ones. It is on these occasions that the appropriate routing to internal and external stakeholders is determined. Both TSNM and OI have information-sharing mechanisms that are selected and used as appropriate to the circumstances. Overarching guidance for information sharing is documented in the TSISP as well as elements of the TSISP that articulate sector stakeholder information-sharing forums and methodologies.

The draft report contained five recommendations with which DHS concurs and has already initiated steps to implement. Specifically, GAO recommended that the Secretary of Homeland Security direct the Assistant Secretary for the Transportation Security Administration:

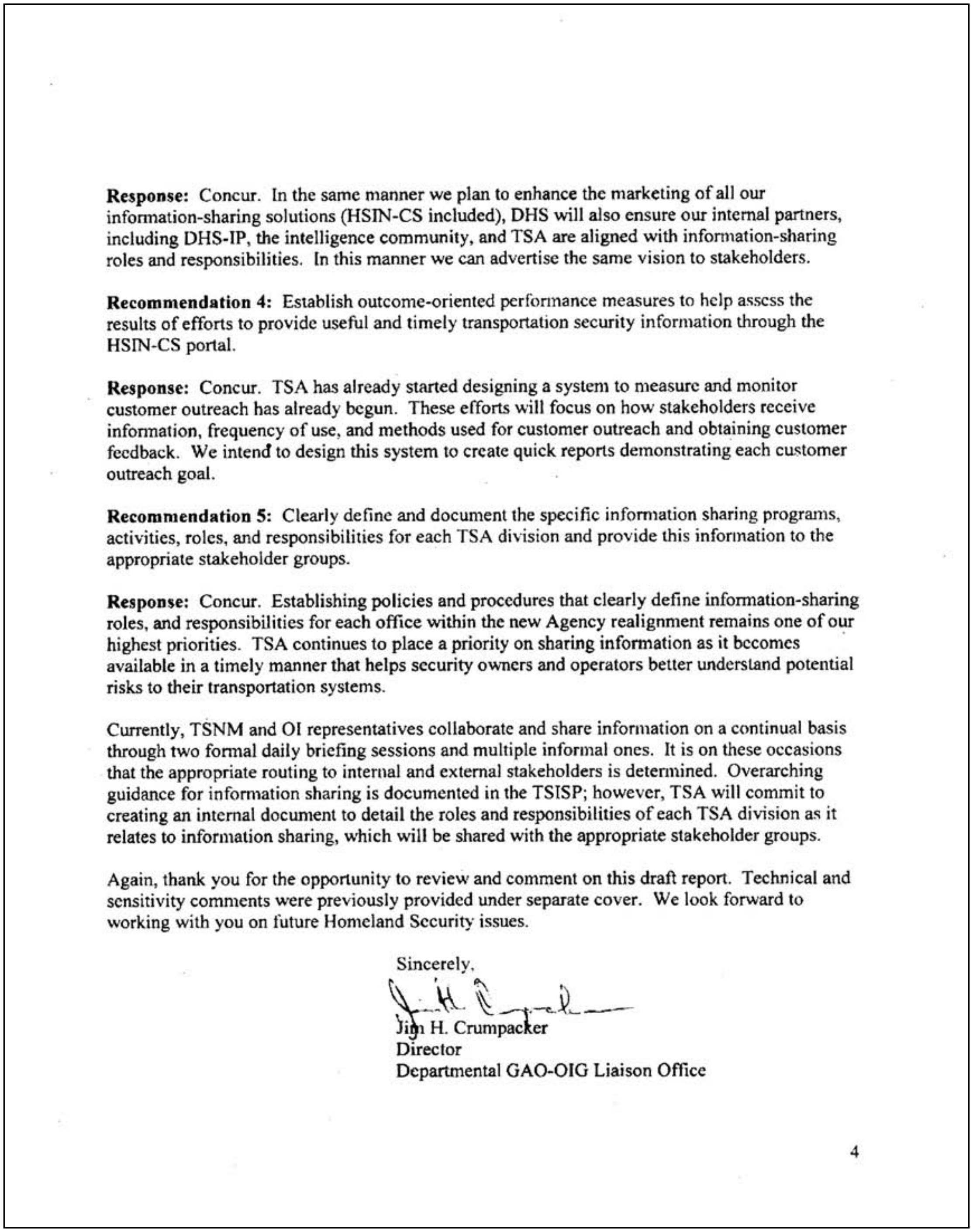
Recommendation 1: To the extent possible, address the need expressed by stakeholders by providing more actionable analysis in TSA's transportation security-related information products.

Response: Concur. Since the conclusion of the fieldwork for this report, many DHS products now focus on a threat-level measurability ranging from low to high. In addition to grading threat levels for each mode of transportation, TSA includes trends and tactics, techniques, and procedures in order to help security owners and operators implement more effective countermeasures.

Recommendation 2: In coordination with other DHS components, conduct targeted outreach efforts to aviation, rail, and highway stakeholders to increase the number of transportation stakeholders who are receiving security-related information products and are made aware of security information available through the HSIN-CS portal.

Response: Concur. In collaboration with the DHS Office of Infrastructure Protection (DHS-IP), TSA will continue marketing efforts to aviation, rail, and highway stakeholders to increase awareness of security-related information available not only through HSIN-CS, but also through other information-sharing systems. DHS already implemented multiple information-sharing systems approved by DHS, FBI, NCTC, and ODNI, which disseminate intelligence to stakeholders. Further, since the conclusion of GAO's fieldwork for this review, DHS's strategy has evolved to consider stakeholders' preferred methods of receiving security-related information. For example, TSA now partners with the following systems: HSIN-Intelligence, DSAC, InfraGard, RISSNET, Law Enforcement Online, and NCTC Online. Most recently, TSA conducted a partnership outreach and established a transportation page on the DSAC portal that contains links to the routine notification emails sent out to DSAC members.

Recommendation 3: Coordinate with other DHS components to improve the ability to readily locate information in TSA security-related information sharing products on HSIN-CS.



Response: Concur. In the same manner we plan to enhance the marketing of all our information-sharing solutions (HSIN-CS included), DHS will also ensure our internal partners, including DHS-IP, the intelligence community, and TSA are aligned with information-sharing roles and responsibilities. In this manner we can advertise the same vision to stakeholders.

Recommendation 4: Establish outcome-oriented performance measures to help assess the results of efforts to provide useful and timely transportation security information through the HSIN-CS portal.

Response: Concur. TSA has already started designing a system to measure and monitor customer outreach has already begun. These efforts will focus on how stakeholders receive information, frequency of use, and methods used for customer outreach and obtaining customer feedback. We intend to design this system to create quick reports demonstrating each customer outreach goal.

Recommendation 5: Clearly define and document the specific information sharing programs, activities, roles, and responsibilities for each TSA division and provide this information to the appropriate stakeholder groups.

Response: Concur. Establishing policies and procedures that clearly define information-sharing roles, and responsibilities for each office within the new Agency realignment remains one of our highest priorities. TSA continues to place a priority on sharing information as it becomes available in a timely manner that helps security owners and operators better understand potential risks to their transportation systems.

Currently, TSNM and OI representatives collaborate and share information on a continual basis through two formal daily briefing sessions and multiple informal ones. It is on these occasions that the appropriate routing to internal and external stakeholders is determined. Overarching guidance for information sharing is documented in the TSISP; however, TSA will commit to creating an internal document to detail the roles and responsibilities of each TSA division as it relates to information sharing, which will be shared with the appropriate stakeholder groups.

Again, thank you for the opportunity to review and comment on this draft report. Technical and sensitivity comments were previously provided under separate cover. We look forward to working with you on future Homeland Security issues.

Sincerely,

Jim H. Crumpacker
Director
Departmental GAO-OIG Liaison Office

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

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

Staff Acknowledgments

In addition to the contact named above, individuals making key contributions to this report include Jessica Lucas-Judy, Assistant Director; Kevin Heinz, Analyst in Charge; Adam Anguiano; Katherine Davis; Tracey King; Stan Kostyla; Landis Lindsey; Ying Long; Lauren Membreno; Michael Silver; and Meg Ullengren.

Related GAO Products

Department of Homeland Security: Progress Made and Work Remaining in Implementing Homeland Security Missions 10 Years after 9/11. GAO-11-881. Washington, D.C.: September 7, 2011.

Information Sharing Environment: Better Road Map Needed to Guide Implementation and Investments. GAO-11-455. Washington, D.C.: July 21, 2011.

Rail Security: TSA Improved Risk Assessment but Could Further Improve Training and Information Sharing. GAO-11-688T. Washington, D.C.: June 14, 2011.

High Risk Series: An Update. GAO-11-278. Washington, D.C.: February 2011.

Public Transit Security Information Sharing: DHS Could Improve Information Sharing through Streamlining and Increased Outreach. GAO-10-895. Washington, D.C.: September 22, 2010.

Information Sharing: Federal Agencies Are Sharing Border and Terrorism Information with Local and Tribal Law Enforcement Agencies, but Additional Efforts Are Needed. GAO-10-41. Washington, D.C.: December 18, 2009.

Information Sharing Environment: Definition of the Results to Be Achieved in Improving Terrorism-Related Information Sharing Is Needed to Guide Implementation and Assess Progress. GAO-08-492. Washington, D.C.: June 25, 2008.

Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information. GAO-06-385. Washington, D.C.: March 17, 2006.

Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors. GAO-04-780. Washington, D.C.: July 9, 2004.

(440879)

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 website (www.gao.gov). Each weekday afternoon, GAO posts on its website 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 website, 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.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: 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