United States Government Accountability Office

GAO

Report to Congressional Committees

September 2010

PUBLIC TRANSIT SECURITY INFORMATION SHARING

DHS Could Improve Information Sharing through Streamlining and Increased Outreach

GAO-10-895

September 2010

PUBLIC TRANSIT SECURITY INFORMATION SHARING

DHS Could Improve Information Sharing through Streamlining and Increased Outreach

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-10-895, a report to congressional committees

Why GAO Did This Study

The Transportation Security Administration (TSA), in the Department of Homeland Security (DHS), is committed to sharing information with public transit agencies. The Implementing Recommendations of the 9/11 Commission Act directed GAO to report on public transit information sharing. This report describes (1) the primary mechanisms used to share security information with public transit agencies; and evaluates (2) public transit agencies' satisfaction with federal efforts to share security-related information (e.g., security threats) and opportunities to improve these efforts; and (3) the extent to which DHS has identified goals and measures for sharing information. GAO surveyed 96 of the 694 U.S. public transit agencies based on 2008 ridership and received 80 responses. The 96 public transit agencies surveyed represent about 91 percent of total 2008 ridership. GAO also reviewed documents, such as DHS's *Information Sharing Strategy*, and interviewed agency officials.

What GAO Recommends

GAO recommends that DHS, among other things, (1) establish time frames for its working group to develop options for improving information sharing, including assessing opportunities to streamline mechanisms and conducting targeted outreach; and (2) establish time frames for developing goals and outcome-oriented measures of results. DHS concurred. GAO is issuing an electronic supplement with this report—GAO-10-896SP—which provides survey results.

View GAO-10-895 or key components.
For more information, contact Stephen M. Lord at (202) 512-4379 or LordS@gao.gov.

What GAO Found

According to the American Public Transportation Association (APTA)—which represents the public transit industry—and TSA officials, the Public Transportation Information Sharing and Analysis Center (PT-ISAC) and the public transit subportal on DHS's Homeland Security Information Network (HSIN-PT) were established as primary mechanisms for sharing security-related information with public transit agencies. The public transit agencies GAO surveyed also cited additional mechanisms for obtaining such information, including other public transit agencies. Further, in March 2010 TSA introduced the Transportation Security Information Sharing and Analysis Center (TS-ISAC), which is a subportal on HSIN focused on sharing security-related information with transportation stakeholders.

Seventy-five percent of the public transit agencies GAO surveyed reported being generally satisfied with the security-related information they received; however, federal efforts to share security-related information could be improved. Specifically, three-fourths of public transit agencies reported being either very satisfied or somewhat satisfied with the information they received. Public transit agencies also reported that among the 12 most frequently cited mechanisms, they were the least satisfied with HSIN in terms of general satisfaction (19 of 33) and for each of six dimensions of quality—relevance, validity, timeliness, completeness, actionability, and ease of use. Twenty-four survey respondents also cited the need to streamline the information they received. GAO identified the potential for overlap between the PT-ISAC, the HSIN-PT, and the TS-ISAC, which all communicate similar unclassified and security-related information to public transit agencies. Federal and transit industry officials that GAO interviewed reported the need to streamline information sharing. Moreover, a greater proportion of survey respondents who were unaware of the PT-ISAC or HSIN were from midsize agencies, nonrail agencies, and those without their own police department. Federal and industry officials formed a working group to assess the effectiveness of information-sharing mechanisms, including developing options for streamlining these mechanisms. TSA officials stated that these options will also impact future outreach activities; however, no time frame has been established for completing this effort. Establishing such a time frame could help to ensure that this effort is completed.

DHS and TSA have established goals and performance measures for some of their information-sharing activities to help gauge the effectiveness of their overall information-sharing efforts; however, they have not developed goals and outcome-oriented measures of results of activities for the mechanisms established as primary information sources for the public transit industry. TSA officials acknowledged the importance of establishing such goals and measures, but were unable to provide time frames for doing so. Establishing time frames for developing goals and outcome measures, once the working group effort is complete, could assist TSA in gauging the effectiveness of its efforts to share information with public transit agencies.

Contents

Tables

Figure

Abbreviations

APTA	American Public Transportation Association
DHS	Department of Homeland Security
DOJ	Department of Justice
DOT	Department of Transportation
FBI	Federal Bureau of Investigation
FOUO	For Official Use Only
FTA	Federal Transit Administration
GCC	Government Coordinating Council
HSIN	Homeland Security Information Network
HSIN-CS	Homeland Security Information Network Critical Sectors portal
HSIN-PT	Homeland Security Information Network public transit subportal
I&A	Office of Intelligence and Analysis
IP	Office of Infrastructure Protection
JTTF	Joint Terrorism Task Force
NIPP	National Infrastructure Protection Plan
NPPD	National Protection and Programs Directorate
PT-ISAC	Public Transportation Information Sharing and Analysis Center
SBU	Sensitive but Unclassified
SCC	Sector Coordinating Council
TSA	Transportation Security Administration
TSA-OI	Transportation Security Administration Office of Intelligence
TS-ISAC	Transportation Security Information Sharing and Analysis Center
TSISP	Transportation Security Information Sharing Plan
TSOC	Transportation Security Operations Center
TSNM	Transportation Sector Network Management

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

September 22, 2010

Congressional Committees

Public transit systems provided 10.2 billion passenger trips in the United States in calendar year 2009.[1] To date, U.S. public transit systems have not been successfully attacked by terrorists. However, the February 2010 guilty plea by Najibullah Zazi for, among other things, conspiring to detonate explosives in the New York City subway system highlighted the vulnerability of public transit agencies and the importance of the federal government to share quality security-related information with the public transit industry.[2] The Homeland Security Act of 2002 and the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act)—assigned the Department of Homeland Security (DHS) responsibility for sharing information related to terrorism and homeland security with its federal, state, tribal, local, and private sector homeland security partners.[3]

Since the terrorist attacks of September 11, 2001, the federal government, including DHS, has taken a number of actions to enhance the security of transportation systems. These actions include improving information sharing with its critical sector stakeholders, which is highlighted in the 2008 *Department of Homeland Security Information Sharing Strategy*,

[1] A passenger trip is defined as the number of passengers who board public transportation vehicles. Passengers are counted each time they board vehicles no matter how many vehicles they use to travel from their origin to their destination. Ridership data were reported by the American Public Transportation Association (APTA) for calendar year 2009. This figure does not include those passengers who rode passenger ferries during calendar year 2009.

[2] For the purposes of this report, we define security-related information as information that provides: (1) details on various security threats, including a terrorist attack; terrorist, cyber, and technical threats, or other security incident or suspicious activity pertaining to a specific entity or industry; (2) analysis of the threat and instructions and recommendations on security measures an entity should take to protect its people and resources from a terrorist attack, threat, or other security incident; (3) awareness of the threat environment, notably capabilities, tactics, and techniques; (4) awareness of system vulnerabilities and consequences of a terrorist attack or other security incident; or (5) U.S. and international security practices and lessons learned. TSA and APTA both agreed with this definition.

[3] See Pub. L. No. 107-296, § 201, 116 Stat. 2135, 2145-49 (2002); Pub. L. No. 110-53, title V, 121 Stat. 266, 306-35 (2007). Among other things, the 9/11 Commission Act mandates that DHS require all public transit agencies considered to be high risk to participate in the PT-ISAC and encourage all other transit agencies to use it.

as well as the 2009 *National Infrastructure Protection Plan* (NIPP).[4] To help facilitate information sharing with the public transit industry, DHS and the Transportation Security Administration (TSA) have created and funded a number of mechanisms, including the Public Transportation Information Sharing and Analysis Center (PT-ISAC), which is administered by the American Public Transportation Association (APTA).[5] The PT-ISAC was created under the direction of the Department of Transportation (DOT) in 2003 and is currently funded by TSA via DOT's Federal Transit Administration (FTA).[6] In addition to DHS, other federal agencies, such as the Department of Justice's (DOJ) Federal Bureau of Investigation (FBI) and FTA, have also taken action to enhance their efforts to share security-related information with public and private stakeholders, including public transit agencies.

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.[7] In January 2005, we designated establishing effective mechanisms for sharing terrorism-related information to protect the homeland a high-risk area because the

[4] For additional information on the strategies, plans, and reports designed to enhance the sharing of terrorism-related information among federal, state, local, and tribal agencies, and the private sector, see appendix II.

[5] APTA's members serve more than 90 percent of persons using public transportation in the United States and Canada. APTA is also responsible for setting policy, directing activity, validating membership, and advocating for the value of the PT-ISAC.

[6] The PT-ISAC is funded by the federal government through a cooperative agreement with APTA. The 9/11 Commission Act requires DHS to fund the PT-ISAC. However, because FTA already had a process in place to provide funds to the PT-ISAC, TSA signed an interagency agreement with FTA to reimburse its PT-ISAC expenses. The TSA/FTA interagency agreement also contained several tasks for the PT-ISAC, including managing the content, controlling access, enhancing the user-friendliness of the public transit subportal on the Homeland Security Information Network (HSIN-PT), and providing TSA with quarterly operational and financial reports. APTA agreed to fulfill these additional responsibilities by signing its cooperative agreement with FTA. In 2009, DHS provided $600,000 for the PT-ISAC to operate for a period of 18 months.

[7] See, for example, GAO, *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. 2009), *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. 2006), and *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 2008).

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.[8]

As mandated by section 1410 of the 9/11 Commission Act, this review assesses the role of the PT-ISAC and other related federal mechanisms for sharing security-related information within the public transit industry.[9] Specifically, our report addresses the following questions:

- What are the primary mechanisms established or funded by the federal government to share security-related information with public transit agencies?
- To what extent are public transit agencies satisfied with federal efforts to share security-related information, and how, if at all, can these efforts be improved?
- To what extent has DHS identified goals for sharing security-related information with public transit agencies and developed measures to gauge its progress in meeting those goals?

To identify the mechanisms established or funded by the federal government to serve as primary information sources for public transit agencies, we reviewed and assessed relevant documentation, such as the Homeland Security Information Network (HSIN) Program Management Plan and DHS's Information Sharing Strategy. We interviewed officials from DHS components including the Office of Infrastructure Protection (IP) within the National Protection and Programs Directorate (NPPD), the Office of Intelligence and Analysis (I&A), the U.S. Coast Guard, and TSA, as well as officials from FTA and the FBI to discuss the mechanisms they use to share security-related information with public transit agencies.[10] We also conducted site visits, or held teleconferences, with security and management officials from a nonprobability sample of 27 public transit agencies across the nation to determine which mechanisms are most routinely used by these agencies to obtain security-related information.

[8] GAO, *High Risk Series: An Update*, GAO-09-271 (Washington, D.C.: Jan. 2009).

[9] Pub. L. No. 110-53, § 1410(c), 121 Stat. 266, 413 (2007).

[10] We did not include Amtrak in the scope of this review because federal transportation law excludes Amtrak in its definition of public transportation. 49 U.S.C. § 5302.

These transit agencies were selected to reflect broad representation in size, location, transportation mode, and law enforcement presence and represent about 63 percent of the nation's total public transit ridership based on information we obtained from FTA's National Transit Database. Because we selected a nonprobability sample of transit agencies to interview, the information obtained cannot be generalized to all transit agencies. However, the interviews provided illustrative examples of the perspectives of various transit agencies about federal government information-sharing mechanisms and corroborated information we gathered through other means.

To assess the extent to which public transit agencies are satisfied with federal efforts to share quality security-related information and related opportunities for improvement, in March and April 2010, we surveyed 96 of the 694 U.S. public transit agencies on their satisfaction with information-sharing efforts.[11] The 96 public transit agencies surveyed represent about 91 percent of total 2008 ridership. For the purposes of this survey, we defined the six aspects of quality security-related information as (1) relevance (i.e., is the information sufficiently relevant to be of value to a public transit agency?); (2) validity (i.e., is the information accurate?); (3) timeliness (i.e., is information received in a timely manner?); (4) completeness (i.e., does the information contain all the necessary details?); (5) actionability (i.e., would the information allow a public transit agency to change its security posture, if such a change was warranted?); and (6) access/ease of use (i.e., is information available through this mechanism easy to obtain?).[12] Out of the original population of 96 transit agencies, we received completed questionnaires from 80 respondents—a response rate of 83 percent; however, not all respondents provided answers to every question. To develop the survey instrument, we conducted pretest interviews with four public transit agencies and obtained input from our survey experts. However, since we surveyed a

[11] The total number of public transit agencies reflects those agencies that reported data to the National Transit Database in 2008. We surveyed 96 of the top 100 agencies as measured by fiscal year 2008 ridership. We omitted two agencies after learning these two entities are each comprised of multiple smaller transit agencies that, for ease of reporting, consolidate their annual ridership totals in the National Transit Database. In addition, we omitted two other agencies after learning that the security points-of-contact at these two agencies were also responsible for security at two other top-100 agencies and consequently already received our survey.

[12] We developed these six dimensions of quality in consultation with GAO methodologists as well as public transit agency officials during survey pretests.

non-probability sample of public transit agencies, the results cannot be used to make inferences about the entire population of public transit agencies, but provided us with additional insights. 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-10-896SP. To further address this question, we assessed relevant documentation, including interagency agreements between TSA and FTA, as well as marketing materials on the Transportation Security Information Sharing and Analysis Center (TS-ISAC). We also interviewed APTA, PT-ISAC, TSA, FBI, FTA, and DHS Office of Operations, Coordination, and Planning officials to discuss efforts to streamline existing information-sharing mechanisms, oversee the results of the PT-ISAC, and conduct outreach on various information-sharing mechanisms. We compared these efforts to internal control standards, as well as our previous work on the need to consolidate redundant information systems and target outreach efforts. In addition, we interviewed select public transit agencies and included questions in our Web-based survey of public transit agencies on the various information-sharing mechanisms available to them.

To assess the extent to which DHS has identified goals for sharing information with public transit agencies and developed measures to gauge its progress in meeting those goals, we reviewed the *DHS Annual Performance Report, Fiscal Years 2008 through 2010*, TSA's *Transportation Security Information Sharing Plan* (TSISP), and available performance measures for fiscal years 2007 through 2010 related to information-sharing efforts with public transit agencies and compared them to leading management practices and our previous work on program assessments.[13] We also interviewed relevant DHS and TSA officials to obtain information on their efforts to revise and develop performance measures and goals for this area of information sharing and to obtain feedback from public transit agencies on their satisfaction with the security-related information they receive. In addition, we compared TSA's efforts to evaluate their information-sharing efforts with guidance on

[13] See GAO, *Executive Guide: Effectively Implementing the Government Performance and Results Act*, GAO/GGD-96-118 (Washington, D.C.: June 1996).

performance measurement contained in our previous reports.[14] Appendix I provides more details about our objectives, scope, and methodology.

We conducted this performance audit from August 2009 through September 2010 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Overview of the U.S. Public Transit Systems

The nation's transportation system is a vast, interconnected network of diverse modes. Key modes of transportation include aviation, freight rail, highway, maritime, transit, and pipeline. The nation's public transit system includes multiple-occupancy vehicle services designed to provide regular and continuing general or special transportation to the public, such as transit buses, light rail, commuter rail, subways, and waterborne passenger ferries. According to APTA, buses are the most widely used form of transit, providing almost two-thirds of all passenger trips. Light rail systems are typically characterized by lightweight passenger rail cars that operate on track that is not separated from vehicular traffic. Commuter rail systems typically operate on railroad tracks and provide regional service (e.g., between a city and adjacent suburbs). Subway systems, like the Metropolitan Transportation Authority's New York City Transit, typically operate on fixed heavy lines within a metropolitan area and have the capacity for a heavy volume of traffic. Waterborne passenger ferries provide a link across many of the nation's waterways and, in some cases, present drivers with an alternative travel option. Public transit systems in the United States are typically owned and operated by public sector entities, such as state and regional transportation authorities. In addition, while some transit agencies rely on their local police department

[14] GAO, *Highway Infrastructure: Federal Efforts to Strengthen Security Should Be Better Coordinated and Targeted on the Nation's Most Critical Highway Infrastructure*, GAO-09-57 (Washington, D.C.: Jan. 2009), *Defense Logistics: Improving Customer Feedback Program Could Enhance DLA's Delivery of Services*, *GAO-02-776* (Washington, D.C.: Sept. 2002).

to secure their systems, others, such as the Bay Area Rapid Transit system in San Francisco, have established their own dedicated police department.

Mass transit and passenger rail systems carry a high number of passengers every day and are open and fully accessible. Multiple stops and transfers lead to high passenger turnover, which is difficult to monitor effectively, and a terrorist attack on public transit systems could result in a large number of casualties. While there have been no successful terrorist attacks against U.S. public transit systems to date, terrorist attacks on public transit systems around the world, such as the March 2010 subway bombings in Moscow, Russia, and the recent plot to detonate explosives on the New York City subway system, illustrate the potential threat to public transit systems.

Multiple Stakeholders Have Responsibility for Sharing Security-Related Information with Public Transit Agencies

Securing the nation's public transit systems is a shared responsibility requiring coordinated action on the part of federal, state, and local governments; the private sector; and passengers who ride these systems. A component of this shared responsibility is ensuring that those within the private and public sector have access to quality security-related information to enhance prevention and protection efforts. DHS is the lead department involved in securing the nation's homeland. As required by the Homeland Security Act of 2002, the department is responsible for coordinating homeland security efforts across all levels of government and throughout the nation, including with federal, state, tribal, local, and private sector homeland security stakeholders.[15]

The Aviation and Transportation Security Act established TSA as the federal agency with primary responsibility for securing the nation's transportation systems.[16] As part of this responsibility, TSA serves as the lead DHS component responsible for assessing intelligence and other information to identify individuals who pose a threat specifically to transportation security and to coordinate countermeasures with other federal agencies to address such threats. TSA is also charged with serving

[15] See Pub. L. No. 107-296, § 102(c), 116 Stat. 2135, 2143 (2002). The Homeland Security Act also transferred TSA from DOT to DHS.

[16] Aviation and Transportation Security Act, Pub. L. No. 107-71, § 101(a), 115 Stat. 597 (2001).

as the sector-specific agency for the transportation community.[17] Within TSA, several offices, including the Office of Transportation Sector Network Management and the Office of Intelligence, play a role in sharing security-related information with transportation stakeholders. In addition to TSA, a number of other entities are responsible for sharing security-related information with internal and external stakeholders, including public transit agencies. Table 1 below provides details on roles and responsibilities of some of the various entities involved in sharing security-related information with public transit agencies.

Table 1: Entities Involved in Sharing Security-Related Information with Public Transit Agencies

Entity	Information sharing role
TSA-Office of Transportation Sector Network Management (TSNM)	Leads federal efforts to protect and secure the nation's transportation systems, with divisions dedicated to each transportation mode, including public transit.[a]
TSA Office of Intelligence (TSA-OI)	Responsible for collecting and analyzing threat information related to the transportation network, which includes all modes of transportation. TSA-OI is also responsible for overseeing the content on the Transportation Security Information Sharing and Analysis Center (TS-ISAC), implemented in March 2010.[b]
DHS Office of Intelligence and Analysis (I&A)	A member of the national intelligence community, DHS I&A is responsible for collecting, analyzing, and disseminating information related to homeland security threats to homeland security stakeholders, including those within the private and public sectors.
DHS Office of Infrastructure Protection (IP)	Within IP, several divisions play a role in sharing security-related information with public transit agencies, including the Homeland Infrastructure Threat and Risk Analysis Center which has analysts dedicated to identifying the risk associated with the transportation sector and sharing that information via associated information products.
DOT's Federal Transit Administration (FTA)	FTA disseminates transit security and threat reports to other federal agencies, including DHS, and transit agencies' representatives. In a 2004 memorandum of understanding (MOU) and a 2005 annex to the MOU, TSA and FTA agreed to coordinate their efforts to share threat information with public transportation stakeholders.
DOT's S-60	DOT's Office of Intelligence, Security and Emergency Response, referred to as S-60, collects, analyzes, and provides security information to both internal DOT and other federal agencies, who in turn share this information with other security stakeholders, including public transit agencies.
FBI	Responsible for protecting and defending the United States from terrorist threats and serving as the nation's principal counterterrorism investigative agency, among other responsibilities. The FBI's Rail Liaison Agents filter and distribute the relevant security-related information to rail transit agencies that they receive from their local Joint Terrorism Task Force (JTTF).[c]

[17] Sector-specific agencies are the federal departments or agencies responsible for infrastructure protection activities in a designated critical infrastructure sector or key resources category.

Entity	Information sharing role
APTA	As the sponsor of the PT-ISAC and the secretary of the Mass Transit Sector Coordinating Council (SCC), APTA plays a key role in sharing security-related information with public transit agencies.[d] APTA also manages the PT-ISAC under a cooperative agreement with FTA.[e]

Source: GAO analysis of DHS, DOT, DOJ, and APTA information.

[a]TSA's TSNM coordinates with the U.S. Coast Guard to secure the maritime sector.

[b]See the Senate committee report accompanying the proposed bill for the fiscal year 2009 DHS appropriations act—S. Rep. No. 110-396, at 66 (2008). In this report, the committee directed TSA to implement the TS-ISAC. Hosted on HSIN, the TS-ISAC contains unclassified Sensitive but Unclassified (SBU) intelligence products and other security-related documents available to vetted transportation security stakeholders.

[c]JTTFs are investigative units consisting of law enforcement and other specialists from federal, state, and local law enforcement and intelligence agencies, led by DOJ and the FBI. JTTFs are located in 100 cities nationwide, including at least one in each of the FBI's 56 main field offices. The National Joint Terrorism Task Force oversees the local JTTFs across the country.

[d]According to TSA, the Long-Distance Rail Government Coordinating Council (GCC) and SCC serve as coordinating bodies to discuss, develop, and refine positions on all matters in transit security. In addition, they streamline the coordination process between government and the transit industry, helping to advance a partnership in developing and implementing security programs.

[e]To carry out the day-to-day operations of the PT-ISAC, APTA contracted with Electronic Warfare Associates – Information and Infrastructure Technologies, Inc., to obtain and analyze primarily open source security information and distribute it to PT-ISAC members on a daily basis.

PT-ISAC and HSIN-PT Were Established to Serve as the Primary Security Information-Sharing Mechanisms for Public Transit Agencies

According to APTA and TSA officials, the PT-ISAC and the public transit subportal on DHS's HSIN (HSIN-PT) were designed to serve as the primary mechanisms for sharing security-related information with public transit agencies. The PT-ISAC, which is implemented by APTA under a cooperative agreement with FTA, was designed to serve as the one stop shop for public transit agencies seeking to obtain security-related information. The PT-ISAC collects, analyzes, and distributes security and threat information from the federal government and open sources on a 24/7 basis. It provides public transit agencies with unclassified and open-source documents obtained from numerous sources, including DOT, DHS, and DOJ. According to PT-ISAC officials, this mechanism disseminates this information through daily E-mails with attachments summarizing and analyzing recent security and cybersecurity information, news, threats, and vulnerabilities within the transportation sector. In addition, the PT-ISAC has a searchable library of government and private security documents, and PT-ISAC analysts hold top secret security clearances. HSIN-PT is also focused on providing security-related information pertaining to the public transit industry. According to DHS officials, HSIN was designed to serve as the department's primary information-sharing

mechanism for the larger homeland security community engaged in preventing, protecting from, responding to, and recovering from all threats, hazards, and incidents under DHS jurisdiction.[18] HSIN is comprised of a network of communities, referred to as communities of interest, such as Intelligence and Analysis, Law Enforcement, Emergency Management, and Critical Sectors (CS).[19] Within HSIN-CS, each of the 18 critical sectors maintains its own site. Under the transportation sector, the public transit mode maintains its own subportal on HSIN.[20] According to TSA officials, HSIN-PT is maintained and populated by mass transit and passenger rail private and government stakeholders. HSIN, including its public transit subportal, is accessible via the Internet, but users must first be vetted against established criteria to obtain a user name and password from DHS to access the network and retrieve information. As an additional feature, HSIN users may elect to receive E-mail alerts that include notices of ongoing events or direct the user to a particular location within HSIN to obtain additional information.

While the PT-ISAC and HSIN-PT are focused on providing security-related information to public transit agencies, the agencies we surveyed did not rely solely on these two mechanisms for their information needs. Figure 1 below illustrates the 12 key information-sharing mechanisms, identified by the agencies we surveyed, that disseminate security-related information to public transit agencies.[21] These mechanisms were cited as sources of

[18] According to DHS, HSIN offers a number of capabilities, including 24/7 access, document libraries, incident reporting, situational awareness and analysis, and discussion boards.

[19] Other HSIN communities of interest include, but are not limited to: Continuity of Operations, Federal Department Agency Planning, and International.

[20] There are 18 critical infrastructure sectors, including Agriculture and Food; Banking and Finance; Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Government Facilities; Information Technology; National Monuments and Icons; Nuclear Reactors, Materials and Waste; Postal and Shipping; Public Health and Healthcare; Transportation Systems; and Water. The HSIN-CS portal contains subportals, including the TS-ISAC and HSIN-PT.

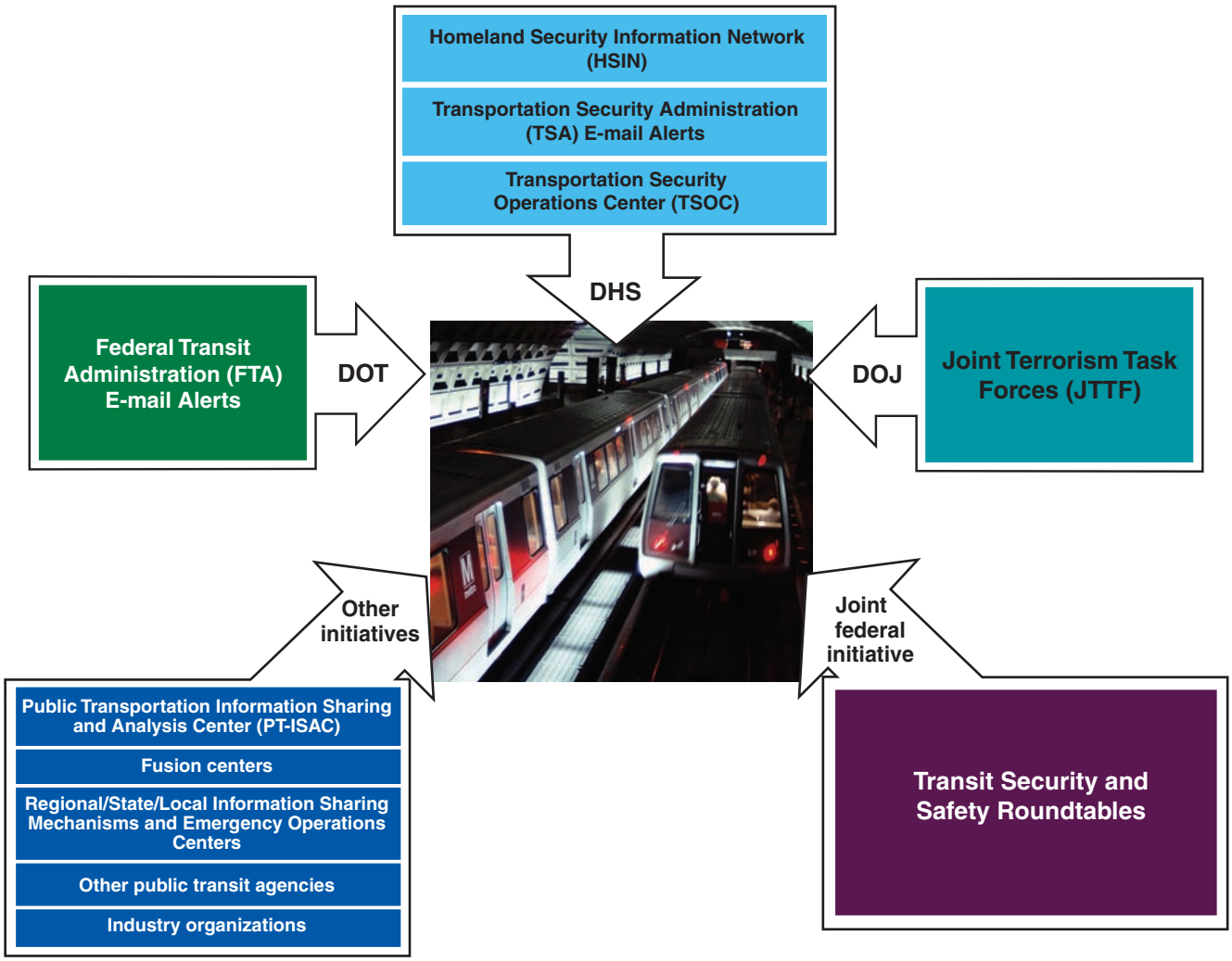
[21] In figure 1, the category "regional/local information sharing mechanisms" includes both "regional/state/local information sharing mechanism" and "regional/state/local emergency operations center," as each was identified as a source of security-related information by over 40 percent of survey respondents.

security-related information by more than 40 percent of the public transit agencies we surveyed.[22]

[22] We included six other mechanisms in our survey that were used by less than 40 percent of public transit agencies. These mechanisms were Law Enforcement Online, DHS Protective Security Advisors, the National Open Source Center, the Federal Protective Service portal, the Regional Information Sharing System-Automated Trusted Information Exchange, and the Transportation Information Sharing System.

Figure 1: Mechanisms Cited Most Frequently by the Public Transit Agencies Surveyed as Sources for Security-Related Information

Interactive features:
Roll your mouse over the name of each information-sharing mechanism for more information. A brief definition of the selected mechanism will appear.
To see the full text, see Table 2.



Source: GAO analysis of information from DHS, DOJ, DOT and public transit agencies; PhotoDisc (photo).

Note: In figure 1, we combine "regional/state/local information-sharing mechanisms" and "regional/state/local emergency operations centers." Both types of mechanisms were identified as sources of security-related information by over 40 percent of survey respondents.

The information-sharing mechanisms described in figure 1 vary by intended users of the mechanism, the type and source of information offered, and how the information is distributed. Table 2 provides additional details on the 12 information-sharing mechanisms public transit agencies cited most frequently as sources for security-related information.

Table 2: Additional Details on the Mechanisms Most Frequently Cited by Surveyed Public Transit Agencies as Sources for Obtaining Security-Related Information

Information sharing mechanism (number of users)[a]	Mechanism description	Mechanism operator/ intended users	Type/source of information offered	How information is distributed (push versus pull system)[b]
PT-ISAC (49)	A 24/7 mechanism with a threat and incident reporting focus. The PT-ISAC collects, analyzes, and distributes security and threat information from the federal government and open sources. It also disseminates information from other industries through its relationship with other ISACs.	This mechanism is administered by APTA and operated by Electronic Warfare Associates – Information and Infrastructure Technologies, Inc. The PT-ISAC is intended to serve the public transit industry.	Unclassified and open source documents including law enforcement bulletins obtained from numerous sources, including federal agencies such as DOT, DHS, and DOJ.	A push system. Daily unclassified E-mails are sent with attachments summarizing and analyzing recent security and cybersecurity information, news, threats, and cited vulnerabilities within the transportation sector.
HSIN (34)	A secure Web-based platform able to facilitate SBU information sharing and collaboration between federal, state, local, tribal, private sector, and international partners.	DHS Office of Operations Coordination and Planning operates this mechanism intended to serve federal, state, local, tribal, private sector, and international partners.	Unclassified and SBU products focused on threats stemming from suicide bombers, suspicious packages, and international security events.	A pull system. Users must log on to the secure network to access information.
FTA E-mail Alerts (65)	The lead emergency coordinator at FTA maintains contact with public transit and law enforcement agencies that mitigate and respond to hazards. The emergency coordinator's network now includes roughly 500 individuals and organizations.	FTA operates this mechanism intended to serve organizations and officials from public transit agencies, federal, state, and local agencies, fusion centers, and law enforcement.	Open source and SBU information sent via daily E-mails that includes breaking news alerts, updates on incidents affecting or disrupting transit operations, police lookouts, counter terrorism information, intelligence bulletins, training and exercise announcements.	A push system. E-mails are provided to public transit officials, organizations, and other individuals within the public transit industry.

Information sharing mechanism (number of users)[a]	Mechanism description	Mechanism operator/ intended users	Type/source of information offered	How information is distributed (push versus pull system)[b]
TSA E-mail Alerts (56)	As a part of its information-sharing efforts, TSA occasionally disseminates E-mails to public transit agencies that include unclassified and SBU security-related information.	TSA operates this mechanism intended to serve the public transit industry.	Unclassified and SBU information such as suspicious incident and situational awareness reports.	A push system. Information is provided via E-mail.
Transportation Security Operations Center (TSOC) (41)	Also known as the Freedom Center, TSOC is a 24/7 operations center that serves as the main point of contact for security-related incidents or crises in all modes of transportation.	TSA operates this mechanism intended to serve all modes of transportation.	SBU information on security-related incidents or crises in all modes of transportation.	A push system. Information is shared with federal TSA stakeholders who, in turn, can choose to share TSOC reports with public transit agencies.
Transit Security and Safety Roundtables (44)	TSA and FTA host roundtables specifically tailored for the nation's largest mass transit and passenger rail agencies to discuss security challenges. These roundtables were formerly held twice a year, but will now be held annually.	FTA and TSA cosponsor these events intended to serve law enforcement police, security chiefs, and safety directors from the nation's largest mass transit and passenger rail agencies.	SBU and open source information shared during presentations and discussions on specific terrorism prevention, response challenges and efforts to develop effective risk mitigation and security enhancements.	A push system. Information is shared during these meetings with public transit officials. A CD with information presented at the roundtables is also distributed to roundtable participants.
Joint Terrorism Task Forces (JTTF) (53)	Small groups of trained, locally based investigators, analysts, linguists, and other specialists from U.S. law enforcement and intelligence agencies. JTTFs are led by the FBI and are designed to combine the resources of federal, state, and local law enforcement.	The FBI operates this mechanism intended to serve all law enforcement critical sectors, including public transit.	SBU and classified information related to counterterrorism, current relevant investigations, suspicious activities, significant events, and threats.	Push systems. Information is shared via secure telephones, E-mail, in person, and secure video teleconferences.
Fusion Centers (39)	A collaborative effort of two or more federal agencies that provide resources, expertise, and information to the center to improve the ability to detect, prevent, and respond to criminal and terrorist activity. DHS provides support to fusion centers through grant funding, technical assistance, training, and data access.	State and local law enforcement or governments operate these mechanisms intended to serve federal, state, and local governments, law enforcement, and the private sector.	SBU and classified information related to homeland security, terrorism, threats, all crimes, and all hazards (such as public health, safety issues or emergencies). DHS and DOJ provide many fusion centers access to their information systems.	Push systems. Information is provided via E-mail, telephone, or in-person.

Information sharing mechanism (number of users)[a]	Mechanism description	Mechanism operator/ intended users	Type/source of information offered	How information is distributed (push versus pull system)[b]
Other Public Transit Agencies (48)	Public transit agencies may receive unclassified security-related information from other public transit agencies on an ad-hoc basis. For example, a large public transit agency may pass along security-related information to a smaller agency in the same geographic region, or security officials at one agency may receive information from officials at other agencies around the country through informal networks.	Public transit industry operates and uses this type of mechanism.	Unclassified information such as suspicious incidents, alerts, and other security information specific to public transit agencies.	Push systems. Informal communication via E-mail, in-person, or teleconference.
Regional/State/ Local Information Sharing Mechanisms and Emergency Operations Centers[c] (47)	In addition to federal information-sharing mechanisms, public transit agencies also reported using regional or local information-sharing mechanisms. These mechanisms were established either individually or in coordination with other local or state entities, such as offices of emergency management, local law enforcement, and other public transit agencies.	Local law enforcement agencies, emergency management agencies or regional working groups operate this type of mechanism intended to serve federal, state, local law enforcement and public transit industry.	Unclassified information on security incidents, alerts, threats, vulnerabilities, and grants.	Although these mechanisms vary by region, the mechanisms described by officials from the 27 public transit agencies we interviewed were push systems that provided information via E-mail, telephone, or in person.
Industry organizations (e.g., APTA) (44)	Industry organizations such as APTA may share security-related information directly with public transit agencies. This information may include, among other things, guidance on improving security and emergency response plans, as well as training opportunities.	Private industry operates this type of mechanism intended to serve the public transit industry.	Unclassified guidance, situational awareness, security alerts, as well as all hazards and safety information.	Push systems. Information is shared during industry conferences, via E-mail, in-person, and teleconferences.

Source: GAO analysis of DHS, DOT, DOJ, PT-ISAC, APTA, and public transit agency information.

[a]The number of users equals the total number of agencies that reported using this mechanism based on survey data. For HSIN, the number in parentheses represents the 34 agencies that indicated they had log-in access to HSIN and had not lost or forgotten their password.

[b]For the purposes of this report, we define a push system as a system that automatically distributes information to users. We define a pull system as a system that requires a user to log on to obtain information.

[c]In table 2, we combined "regional/state/local information-sharing mechanism" and "regional/state/local emergency operations center," although both mechanisms were identified as sources of security-related information by over 40 percent of survey respondents. Specifically, according to our survey results, 47 agencies reported using regional/local information-sharing mechanisms and 38 agencies reported using regional emergency operations centers to receive security-related information.

Although all of these mechanisms are used by some segment of the public transit agencies we surveyed to obtain security-related information, access to the information disseminated through the mechanisms illustrated in table 2 may vary by, among other factors, whether the transit agencies have a dedicated police department, the size of transit agency, and accessibility of the information. For example, some public transit agencies with a dedicated police department receive security-related information through their law enforcement representative on the local JTTF.[23] According to FBI officials, public transit agencies that do not have a dedicated police department are less likely to receive information from the JTTF. In addition, the Transit Security and Safety Roundtables are specifically tailored for the nation's largest mass transit and passenger rail agencies, typically those ranked within the top 50 or 60 by ridership. Smaller transit agencies are less likely to receive information disseminated through this mechanism since they are typically not invited to participate in these roundtables. Also, of the mechanisms identified by the public transit agencies we interviewed and surveyed, all but one send information directly to transit agencies instead of requiring users to log on to a system to retrieve information ("push" vs. "pull").

In addition to the information-sharing mechanisms identified in table 2, TSA-OI implemented its TS-ISAC in March 2010 as another means for sharing security-related information with the transportation industry, including public transit agencies.[24] Specifically, TSA's vision for the TS-ISAC is to serve as the one stop shop to obtain TSA-OI reports and documentation, such as SBU intelligence products and other documents from other transportation security partners and stakeholders. The TS-ISAC aims to enhance collaboration between operators, law enforcement personnel, and security directors from all transportation modes. Similar

[23] JTTFs are small groups of trained, locally based investigators, analysts, linguists, and other specialists from U.S. law enforcement and intelligence agencies.

[24] According to TSA, the major functions of the TS-ISAC include: (1) dissemination of TSA-OI products; (2) e-mail alerts when new information is available on the site; (3) repository of transportation security information; and (4) collaboration with stakeholders. The TS-ISAC was not fully implemented when we conducted our electronic survey of public transit agencies, and therefore data were not collected on this mechanism.

to HSIN-PT, the TS-ISAC is a subportal of HSIN-CS, and therefore users must have a HSIN password to access it.[25] Once access is obtained, TS-ISAC users can set up alerts to be notified when a new document has been posted to the site.

Public Transit Agencies We Surveyed Were Generally Satisfied with Federal Efforts to Share Security-Related Information, but Opportunities Exist to Improve These Efforts

Large Transit Agencies and Rail Agencies Were Generally More Satisfied with Information-Sharing Efforts Than Midsized Agencies and Non-Rail Agencies

Our survey results indicate that public transit agencies' satisfaction with the security-related information they received varied with the type of transportation service provided and whether the agency was large or midsized. As highlighted in table 3 below, three-fourths of public transit agencies that responded to this question in our survey (57 of 76) were generally satisfied with the security-related information they received, while less than one-sixth (11 of 76) were generally dissatisfied.[26] The agencies that provide heavy rail, light rail, or commuter rail service (rail agencies) were generally more satisfied with the information they received than the agencies that provide bus or ferry service, but not rail service

[25] According to DHS IP, HSIN-PT users are automatically users of the TS-ISAC, as well as HSIN-CS.

[26] Although 80 public transit agencies responded to our survey, not all respondents provided answers to every question. We use the term generally satisfied to describe agencies that indicated they were either "very satisfied" or "somewhat satisfied" with the information they receive. Similarly, we use the term generally dissatisfied to describe agencies that indicated they were either "very dissatisfied" or "somewhat dissatisfied" with the information they receive.

(non-rail agencies). Specifically, most rail agencies (30 of 36) were generally satisfied with the security-related information they received, as opposed to approximately two-thirds (27 of 40) of non-rail agencies.

In addition, the larger agencies we surveyed were generally more satisfied with security-related information-sharing than the midsized agencies.[27] Specifically, nearly all of the large agencies that responded to the survey (14 of 15) were generally satisfied with the security-related information they received, and nearly half (7 of 15) were "very satisfied." By contrast, 43 of 61 midsized agencies were generally satisfied with the information they received, and less than one-sixth (10 of 61) were "very satisfied." Table 3 illustrates public transit agencies' overall satisfaction with the security-related information they received.

Table 3: Public Transit Agencies' Overall Satisfaction with Security-Related Information

Overall satisfaction with security-related information?	Type of public transit agency(number of agencies)				
		Type of service		Size of agency	
	All agencies	Rail agencies	Non-rail agencies	Large agencies	Midsized agencies
Very satisfied	17	12	5	7	10
Somewhat satisfied	40	18	22	7	33
Neither satisfied nor dissatisfied	7	1	6	-	7
Somewhat dissatisfied	9	4	5	1	8
Very dissatisfied	2	1	1	-	2
No opinion / do not know	1	-	1	-	1
Subtotal	76	36	40	15	61
No response	4	3	1	-	4
Total	**80**	**39**	**41**	**15**	**65**

Source: GAO analysis of survey responses.

The agencies we surveyed reported using several different mechanisms to receive security-related information, and in general they were satisfied

[27] For the purpose of this report, large agencies are defined as agencies in our survey sample that had at least 99 million riders in fiscal year 2008. Large agencies had a mean ridership of 400 million in fiscal year 2008, with a range of 99.6 million to 3.34 billion. Midsized agencies are defined as agencies in our survey sample for which fiscal year 2008 ridership was less than 99 million. Midsized agencies had a mean ridership of 29.0 million in fiscal year 2008, with a range of 9.85 million to 87.2 million. We did not survey small agencies (i.e., agencies with less than 9.85 million riders in fiscal year 2008), so they are not included in our analysis.

with the information they received through these mechanisms. Of the mechanisms included in the survey, 12 were used by or accessible to at least 40 percent of the agencies that responded to the survey. The two mechanisms most often cited were E-mail alerts from FTA officials (65 of 76) and E-mail alerts from TSA officials (56 of 76); overall general satisfaction with these two mechanisms was 86 percent and 74 percent, respectively. Transit Security and Safety Roundtables were the highest-rated mechanism for overall general satisfaction, with 33 of 36 agencies generally satisfied.[28] With respect to information relevance, validity, and timeliness—three of the six dimensions of quality we included in the survey—regional emergency operations centers received the highest general satisfaction ratings. For actionable information, respondents rated the information they received from other public transportation systems the highest for general satisfaction (28 of 33). Among the 12 most frequently cited mechanisms, public transit agencies were the least satisfied with HSIN, both in terms of overall general satisfaction (19 of 33) and for each of the six dimensions of quality. Public transit agencies in our survey viewed the PT-ISAC more favorably than HSIN; approximately three-fourths (37 of 49) of PT-ISAC users indicated they were generally satisfied with the security-related information they received from this mechanism. See appendix III for additional data on public transit agencies' satisfaction with individual information-sharing mechanisms.

Public transit agencies also expressed their views on the "cross-sector" information they receive.[29] Most agencies that responded to our survey indicated that receiving cross-sector information is important or very important (63 of 78), and this view was shared by both rail and non-rail agencies. However, these two groups characterized differently the amount of cross-sector information they received. Specifically, approximately half of responding rail agencies indicated that they received "about the right amount" of cross-sector information (18 of 37). The remaining rail agencies either wanted to receive additional cross-sector information (7 of 37) or felt that they already received too much (10 of 37).[30] Conversely,

[28] Transit Security and Safety Roundtables are generally open to the nation's largest mass transit and passenger rail agencies. As such, not all of the agencies we surveyed had access to these meetings.

[29] "Cross-sector information" is information that directly pertains to (1) critical infrastructure sectors outside of the transportation sector, or (2) other transportation modes within the transportation sector that also could be relevant to public transit agencies.

[30] Two rail agencies did not provide a response to this question.

about half of non-rail agencies (22 of 41) reported receiving "too little" or "far too little" cross-sector information. Rail and non-rail agencies also differed with respect to their satisfaction with cross-sector information. Approximately two-thirds of rail agencies that responded to this question (24 of 37) were generally satisfied with cross-sector information, whereas less than half of non-rail agencies (16 of 41) were generally satisfied. See table 4 for public transit agencies' views on cross-sector security information sharing.

Table 4: Public Transit Agencies' Survey Responses on Cross-Sector Information

	Type of service provided by public transit agency		
Amount of cross-sector security information?	**All agencies**	***Rail agencies***	***Non-rail agencies***
Far too much	2	2	-
Too much	10	8	2
About the right amount	35	18	17
Too little	21	6	15
Far too little	8	1	7
No opinion / don't know	2	2	-
Subtotal	***78***	***37***	***41***
No response	2	2	-
Satisfaction with cross-sector security information?			
Very satisfied	14	11	3
Somewhat satisfied	26	13	13
Neither satisfied nor dissatisfied	15	4	11
Somewhat dissatisfied	13	7	6
Very dissatisfied	5	1	4
No opinion / do not know	5	1	4
Subtotal	***78***	***37***	***41***
No response	2	2	-
Total	**80**	**39**	**41**

Source: GAO analysis of survey responses.

Opportunities Exist to Streamline Security Information-Sharing Efforts

According to TSA's 2007 Transportation Systems Sector-Specific Plan Mass Transit Modal Annex, a streamlined and effective system to share mass transit and passenger rail information is needed to facilitate information sharing among the federal government and public and private stakeholders.[31] Additionally, in September 2009, we reported that multiple information systems can create redundancies that make it difficult for end users to discern what is relevant and can overwhelm users with duplicative information from multiple sources.[32]

Public transit agencies currently receive similar security-related information from a variety of sources. In addition to identifying the 12 key mechanisms most frequently used by public transit agencies to obtain security-related information, our survey also identified that nearly 80 percent of respondents (63 of 80) used 5 mechanisms or more to receive security information. Further, through interviews with public transit agencies of various sizes around the country, we identified at least 21 mechanisms through which these agencies receive security-related information. Moreover, the Mass Transit SCC/ Transit, Commuter, and Long-Distance Rail Government Coordinating Council (GCC) joint Information Sharing Working Group (SCC/GCC Information Sharing Working Group)—which is cochaired by TSA and comprised of federal and industry stakeholders and was formed to improve information sharing with public transit agencies—compiled a list that includes 59 different information products distributed to public transit agencies by 17 different sources.[33]

[31] TSA developed the Transportation Systems Sector-Specific Plan in 2007 to document the process to be used in carrying out the national strategic priorities outlined in the NIPP and the *National Strategy for Transportation Security*, which outlines the federal government approach to secure the U.S. transportation system from terrorist threats and attacks. The Transportation Systems Sector-Specific Plan contains supporting modal implementation plans for each transportation mode—including mass transit and passenger rail, which provides information on current efforts to secure mass transit and passenger rail—as well as TSA's overall goals and objectives related to mass transit and passenger rail security.

[32] GAO, *Interagency Collaboration: Key Issues for Congressional Oversight of National Security Strategies, Organizations, Workforce, and Information Sharing*, GAO-09-904SP (Washington, D.C.: Sept. 2009).

[33] Formed in 2009, the SCC/GCC Information Sharing Working Group is focused on determining the security-related information needs of public transit agencies, reviewing the current information sharing mechanisms available to these agencies, and identifying services and a format to share information that would best serve their needs. This working group is to develop options for a security-related information sharing system that would be of value to public transit agencies.

We identified the potential for overlap between three mechanisms that are each designed to communicate similar unclassified and SBU security-related information to public transit agencies: the PT-ISAC, the HSIN-PT subportal, and the newly-formed TS-ISAC. According to APTA, the PT-ISAC is intended to be a one stop shop for public transit agencies' information needs. However, according to DHS, the HSIN platform is intended to serve as the agency's primary mechanism for sharing unclassified and SBU information with homeland security stakeholders, and TSA officials stated that the agency intends for the HSIN-PT subportal to be the primary mechanism for sharing such information with public transit agencies. Moreover, the TS-ISAC—which is hosted on HSIN-CS and is intended to serve as a collaborative information-sharing platform for the public transit and other transportation modes—includes unclassified and SBU transportation-related information products produced by TSA-OI. According to TSA officials, the TS-ISAC, which services the larger transportation community, is not intended to compete with or replace HSIN-PT or the PT-ISAC, but in the future it may include a separate Web page that is specific to public transit.

FTA, TSA, APTA, and public transit agency officials we interviewed expressed the desire to streamline information sharing to reduce the volume of overlapping information public transit agencies receive. For example, the then-Acting Manager of TSA's Mass Transit Division stated that the current number of sources available to public transit agencies to receive security-related information is "overwhelming." Additionally, officials from 16 of 27 agencies we interviewed also suggested that information sharing could be improved by reducing redundancies and consolidating existing mechanisms. Our survey of public transit agencies also indicated a desire for a more streamlined approach to information sharing. In an open-ended question asking how information sharing could be improved, 24 of 80 agencies provided comments in favor of consolidating existing information-sharing mechanisms. For example, according to one respondent who favored streamlining the existing mechanisms, "there are so many purported analysis centers pushing out redundant information that an inordinate amount of my time is spent filtering these many reports to find the high-value nuggets." Our interviews and survey data are consistent with the Administration's March 2010 *Surface Transportation Security Priority Assessment*, which recommended, among other things, that TSA implement an approach for sharing transportation security information that provides all relevant threat information and improves the effectiveness of information flow.

Federal and industry stakeholders have efforts under way intended to improve the efficiency of information sharing with public transit agencies and reduce the volume of overlapping information public transit agencies receive. Specifically, TSA, FTA, APTA, and other government and private sector stakeholders are participating in the SCC/GCC Information Sharing Working Group, which is reviewing how the PT-ISAC, the HSIN-PT subportal, the TS-ISAC, and other related information-sharing mechanisms (including direct E-mails from FTA and TSA officials) might be streamlined or consolidated to better serve the public transit industry. This working group is considering, among other things, whether the PT-ISAC could produce a daily (or twice daily) 2 to 3 page unclassified/For Official Use Only (FOUO) information product using open-source information as well as intelligence products from TSA, DHS, and other entities. This would mark a shift in the PT-ISAC's activities, as it would replace a longer information product (10 to 15 pages) the PT-ISAC prepares using primarily open-source information.[34] Working group participants are still debating how this new information product would be disseminated to the public transit industry (e.g., through direct E-mails to public transit agencies, through HSIN-PT, or both), and whether products could be archived on HSIN-PT or another system to facilitate later viewing. In addition, the working group is considering ways to scale back the number of direct E-mails public transit agencies receive, while still maintaining the capability to disseminate information in this manner when necessary.

Participants in this working group have not yet agreed on a path forward to improve information sharing with public transit agencies. As of July 2010, TSA officials stated that the working group had not yet (1) drafted options for improving information sharing with public transit agencies, (2) documented the group's current working proposal, or (3) established a time frame for completing either of these activities. Additionally, the working group has not yet determined how it will incorporate the TS-ISAC into its proposed options. While TSA, through the working group, is assessing, among other things, the extent to which information-sharing

[34] The PT-ISAC also distributes other information products, including a 3 to 4 page cybersecurity information product based on open-source information and the *DHS Daily Open-Source Infrastructure Report* (which is also available through DHS's Web site). In addition, according to PT-ISAC officials, the PT-ISAC also offers its members a searchable library of government and private security documents, as well as access to a consolidated database of information and guidance pertaining to security technology products that are applicable to the public transit industry.

mechanisms can be streamlined, there are no time frames established for completing these efforts. Developing such time frames to guide the working group's activities—including its assessment of opportunities to streamline existing information-sharing mechanisms that target similar user groups with similar information—could assist TSA in completing this important effort.[35]

The PT-ISAC Is Not Completing Agreed-Upon Responsibilities and Tasks

Standards for Internal Control in the Federal Government provide that internal controls should be designed to assure that ongoing monitoring occurs in the course of normal operations.[36] The cooperative agreement between FTA and APTA that provides funding for the PT-ISAC specifies that the ISAC perform several functions related to the HSIN-PT subportal.[37] For example, the agreement states that the PT-ISAC is to control access to the HSIN-PT subportal, manage the information that is available on the subportal, and take steps to enhance its user-friendliness. As specified in the cooperative agreement, TSA and FTA monitor the PT-ISAC's expenditures and activities through quarterly financial and operational reports to help ensure the PT-ISAC fulfills these tasks.[38]

However, while TSA and FTA oversee PT-ISAC expenditures, they are not currently taking steps to ensure that the PT-ISAC performs all of the activities that are specified under the cooperative agreement. For example, the PT-ISAC does not post its analytical products (or other security-related information) to the HSIN-PT subportal, nor has it organized and archived HSIN-PT content to facilitate better access to information, as specified by the agreement. As a result, HSIN-PT is not regularly updated with security-related information, including PT-ISAC analytical products, which could be beneficial to public transit agencies.

[35] We will continue to review these information sharing mechanisms as part of our efforts to address a statutory mandate to identify federal programs and initiatives with duplicative goals and activities. We expect to issue the results of this additional work early in calendar year 2011. See Pub. L. No. 111-139, § 21, 124 Stat. 8, 29-30 (2010).

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

[37] The PT-ISAC's HSIN-related responsibilities are described in a TSA/FTA interagency agreement. APTA agreed to fulfill these requirements by signing its cooperative agreement with FTA.

[38] The PT-ISAC's reporting requirements are described in a TSA/FTA interagency agreement. As noted above, APTA agreed to fulfill these requirements by signing its cooperative agreement with FTA.

TSA, FTA, APTA, and PT-ISAC officials agree that the PT-ISAC is not performing the HSIN-related functions specified in the FTA/APTA cooperative agreement. These officials told us that through the SCC/GCC Information Sharing Working Group, they are reviewing the specific roles and responsibilities of the PT-ISAC—including activities related to the HSIN-PT subportal. However, regardless of whether the working group redefines the PT-ISAC's roles and responsibilities, it is important to ensure that the activities specified in the cooperative agreement are carried out. Taking steps to ensure the PT-ISAC fulfills its responsibilities and completes agreed-upon tasks could help assure TSA and FTA that this mechanism meets the security information needs of public transit agencies.

Awareness and Use of PT-ISAC and HSIN among Some Public Transit Agencies Could Be Increased

In March 2004, we recommended that agencies take actions to better target federal outreach efforts, and internal control standards call for management to ensure adequate means of communicating with external stakeholders who may have a significant impact on agency goals.[39] Security officials at the public transit agencies we surveyed were not always aware of the existence of the PT-ISAC and HSIN, particularly non-rail agencies, midsized agencies, and agencies that do not have their own dedicated police department. For example, of the 80 agencies we surveyed, 23 indicated they did not receive security information from the PT-ISAC and 8 did not know whether they used this mechanism. Moreover, 15 of the 23 agencies that did not receive information from the PT-ISAC had never heard of it (see table 5).[40]

[39] GAO, *Food Stamp Program: Steps Have Been Taken to Increase Participation of Working Families, but Better Tracking of Efforts Is Needed*, GAO-04-346 (Washington, D.C.: March 2004); GAO/AIMD-00-21.3.1.

[40] Our survey results are consistent with the information we obtained through interviews with public transit agencies. Although the majority of the 27 agencies we interviewed receive information from the PT-ISAC, 8 agencies said they do not receive information from this mechanism, and 5 had never heard of it.

Table 5: Awareness and Use of PT-ISAC for Different Categories of Public Transit Agencies

	Does your agency currently receive security-related information from the PT-ISAC?			
Type of agency	**Yes**	**No[a]**	**Do not know**	**Total**
All agencies	49	23	8	80
Dedicated police department	24	4	1	29
No dedicated police department	25	19	7	51
Rail agencies	30	5	4	39
Non-rail agencies	19	18	4	41
Large agencies	14	1	0	15
Mid-sized agencies	35	22	8	65

Source: GAO analysis of survey responses.

[a] Of the 23 agencies that indicated they did not use the PT-ISAC, 15 had never heard of it.

According to FTA officials, the PT-ISAC is meant to serve as a valuable resource for midsized and smaller public transit agencies. However, our survey results indicate that fewer non-rail and midsized agencies received information from the PT-ISAC than rail and large agencies (19 of 41 non-rail and 35 of 65 midsized agencies, as opposed to 30 of 39 rail agencies and 14 of 15 large agencies, respectively). Moreover, nearly all of the agencies we surveyed that had not heard of the PT-ISAC were non-rail agencies (14 of 15), midsized agencies (15 of 15), or agencies without their own dedicated police department (14 of 15).

APTA conducts some PT-ISAC outreach through E-mails and newsletters to its members and other stakeholders, and FTA officials stated that they promote the PT-ISAC at Transit Security and Safety Roundtables. Both APTA and FTA officials agreed, however, on the need for additional outreach to public transit agencies to increase awareness and use of the PT-ISAC. TSA did not provide information on any existing PT-ISAC outreach efforts, but officials stated that the agency's future actions with respect to the PT-ISAC, including outreach activities, will depend on the proposed options that arise from the SCC/GCC Information Sharing Working Group. However, as noted above, there are no time frames for this working group to draft or finalize its proposals for improving information sharing, including who will be responsible for conducting outreach activities for the PT-ISAC or what these activities will entail. Conducting targeted outreach to agencies that are not currently using the PT-ISAC—particularly non-rail agencies, midsized agencies, and agencies that do not have their own dedicated police department—could help to increase awareness and use of this mechanism.

TSA and APTA officials also stated that not all public transit agencies are aware of HSIN and those that are may not view the system as a valuable resource. The results of our survey are consistent with this view and illustrate that public transit agencies' awareness of HSIN could be increased. For example, less than half of public transit agencies (34 of 77) reported that they had log-in access to HSIN and had not lost or forgotten their log-in information (see table 6).

Table 6: Awareness of and Access to HSIN for Different Categories of Public Transit Agencies

	Does your agency currently have log-in access to HSIN?						
Type of agency	**Yes**	**Yes, but lost/forgot log-in information**	**No[a]**	**Do not know**	***Subtotal***	**No response**	**Total**
All agencies	34	13	19	11	*77*	3	**80**
Dedicated police department	17	7	1	2	*27*	2	**29**
No dedicated police department	17	6	18	9	*50*	1	**51**
Rail agencies	20	8	6	3	*37*	2	**39**
Non-rail agencies	14	5	13	8	*40*	1	**41**
Large agencies	9	4	1	1	*15*	0	**15**
Midsized agencies	25	9	18	10	*62*	3	**65**

Source: GAO analysis of survey responses.

[a]Of the 19 agencies that indicated they do not have log-in access to HSIN, 12 reported they had never heard of it.

As with PT-ISAC usage, a greater proportion of large agencies, rail agencies, and agencies that maintain their own dedicated police departments indicated they had log-in access to HSIN and had not lost or forgotten their log-in information (9 of 15 large agencies, 20 of 39 rail agencies, and 17 of 29 agencies with dedicated police departments, as opposed to 25 of 65 midsized agencies, 14 of 41 non-rail agencies, and 17 of 51 agencies without dedicated police departments, respectively). Moreover, our survey also identified that, of the 19 agencies that do not have HSIN access, 12 had never heard of the mechanism, and an additional 11 agencies did not know whether they had access to HSIN. Of the 12 agencies that had never heard of HSIN, nearly all were non-rail agencies (10 of 12), midsized agencies (12 of 12), or agencies without their own dedicated police department (12 of 12).

Multiple entities have a role in conducting outreach to public transit agencies about HSIN. DHS's Office of Operations, Coordination, and Planning is generally responsible for conducting HSIN outreach, but DHS

officials from this office told us that outreach efforts for HSIN-CS, including the HSIN-PT subportal, are under the purview of DHS IP. However, DHS IP officials told us that they are deferring to APTA and TSA (the sector coordinator and sector-specific agency for mass transit, respectively), as described in the NIPP, to conduct outreach to public transit agencies on the HSIN-PT subportal. TSA has conducted some outreach to the public transit industry about HSIN by including HSIN reminders when it distributes security information via E-mail to public transit agencies. However, as table 6 illustrates, past outreach efforts have not resulted in widespread HSIN awareness and use among public transit agencies that we surveyed (particularly midsized agencies, non-rail agencies, and agencies without a dedicated police department), and our survey results suggest that access to HSIN remains a concern.[41] TSA officials stated that the agency recognizes the need for additional outreach to increase public transit agencies' awareness and use of the HSIN-PT subportal and added that future outreach efforts will depend on the proposed options that arise from the SCC/GCC Information Sharing Working Group. However, there are no time frames for this working group to draft or finalize its proposals for improving information sharing.[42] Conducting targeted outreach to agencies that are not currently using HSIN—particularly non-rail agencies, midsized agencies, and agencies that do not have their own dedicated police department—could help to increase awareness and use of this mechanism.

Regarding the newly-formed TS-ISAC, TSA has conducted initial outreach to increase public transit agencies' awareness. For example, TSA distributed a TS-ISAC marketing package via E-mail to transportation stakeholders, and TSA officials stated that the agency is outreaching to other DHS components, state and local stakeholders, and other ISACs (in addition to the PT-ISAC). According to TSA data from April 2010, officials from 46 public transit agencies had been granted access to the public transit Web page of the TS-ISAC within the first 4 weeks of its operation. However, we did not collect data from public transit agencies on their

[41] According to DHS officials, some critical infrastructure sectors are more active on the HSIN platform than others, but the transportation sector, which includes public transit, historically has not been an active user of HSIN. These officials added that enhancing HSIN's value to transportation users by posting useful content and improving accessibility is necessary before outreach efforts can succeed.

[42] DHS officials told us that if APTA and TSA do not increase their outreach efforts for the HSIN-PT subportal, the Office of Infrastructure Protection would assume this responsibility for them.

awareness or use of the TS-ISAC because it was not implemented until March 2010, after we developed our survey. As a result, we could not determine the extent to which outreach efforts have increased awareness and use of the TS-ISAC in the public transit industry.

Concerns with Accessibility, User-Friendliness, and Information Value May Hinder HSIN from Meeting the Security Information Needs of Public Transit Agencies

Standards for Internal Control in the Federal Government call for agencies to ensure adequate means of communicating with external stakeholders that may have a significant impact on agency goals, and effective information technology management is critical to achieving useful, reliable, and continuous communication of information.[43] However, concerns among public transit agencies about HSIN's accessibility may reduce its value as a source of security-related information. Industry officials characterized HSIN as a "pull" system that requires users to log in and extract what is relevant to their agency. Security officials at 11 of 27 public transit agencies we interviewed told us they prefer security information to be "pushed" out to them (e.g., through E-mails, phone calls) instead of having to log into a system to retrieve it themselves. APTA officials stated that public transit security personnel do not have time to log into a "pull" system, such as HSIN, every day and sift through excess information to extract what is relevant to their agency. In addition, when a HSIN password expires (which occurs after 90 days for security reasons) users must call the HSIN help desk to obtain a new one. However, the contact information for the HSIN help desk is not located on the main HSIN log-in page, so users may not know how to get help if they experience log-in challenges. Of the 27 agencies we interviewed, 8 indicated they had experienced problems accessing HSIN.[44] In June 2010, DHS implemented a new agency policy to identify HSIN users that have not accessed the system in 180 days and notify them via E-mail every 3 months instructing them to contact the HSIN help desk to obtain a new password. DHS officials also told us that the phone number for the HSIN help desk would be added to the HSIN log-in page, but the agency had not done so as of August 2010.

In addition to accessibility concerns, certain aspects of HSIN are not user-friendly, and the security-related information available on the HSIN-PT subportal is not always valuable to public transit agencies. Of the 11

[43] GAO/AIMD-00-21.3.1.

[44] Although the majority of agencies we interviewed (19 of 27) did not indicate they had experienced problems accessing HSIN, this is in part because less than half (11 of 27) indicated they use the system to receive security-related information.

agencies we interviewed that had access to HSIN and used it to receive security-related information, 5 reported problems with using the system once they logged in. These problems included configuring E-mail alerts to notify them when information is discovered or changed in a particular area of HSIN (e.g., the HSIN-PT subportal). We experienced similar problems using these E-mail alerts. After setting up alerts to notify us when documents are discovered or changed on the HSIN-PT subportal, we received multiple notifications on a near-daily basis with links to outdated documents, such as job announcements last modified in 2007, a threat advisory for the New York City subway system last modified in 2006, and a map of power outages caused by Hurricane Wilma in 2005. Further, we found that security-related information on HSIN that could be useful to public transit agencies was not always posted to the HSIN-PT subportal. For example, in the days following the Moscow subway bombings in March 2010, certain documents pertaining to the attack were available on the HSIN-CS portal, but did not appear on HSIN-PT, despite their direct relevance to public transit agency users. The E-mail alerts we had set up for HSIN-PT did not notify us of any of this information, which included a document describing heightened security measures a large U.S. public transit agency took in response to the Moscow attack. This information could have been of interest to other public transit agencies, but HSIN-PT users would not have known about it unless they logged into the system without an E-mail prompt, navigated to the HSIN-CS portal, and found the information themselves. Based on our survey results—which indicate that only 3 of 77 agencies use HSIN daily—agencies may not have known that information pertaining to the Moscow bombings was available to them on HSIN.[45]

DHS and TSA agree that the HSIN-PT subportal is not widely used by the public transit industry and that improvements are needed. One such improvement is related to DHS's efforts to develop a replacement system for the HSIN platform, known as HSIN Next Generation. This new system, which DHS began to develop in 2008, is intended to provide increased security and access to SBU information for public transit agencies and other user communities, including law enforcement, intelligence, immigration, and emergency and disaster management. According to DHS officials, the agency intends to move the subportals on HSIN-CS, including

[45] In our survey, 34 public transit agencies indicated they (1) have access to HSIN and (2) have not lost or forgotten their passwords. Of these 34 agencies, half (17) use the system less than once a month or never.

HSIN-PT, to the new HSIN Next Generation platform during the last quarter of calendar year 2010.[46] Taking steps to ensure public transit agencies can access and readily use HSIN—and ensuring the HSIN-PT subportal contains security-related information that is of value to these agencies—could help DHS improve HSIN's capacity to meet public transit agencies' security-related information needs.

[46] In October 2008, we reported that DHS needed to strengthen program management controls for HSIN Next Generation and recommended that the agency should, among other activities, staff the program office appropriately; ensure user requirements are gathered, analyzed, and validated; and identify key project risks and develop risk mitigation plans. We further recommended that DHS implement these controls before it moves HSIN users (such as public transit agencies) to HSIN Next Generation. As of July 2010, DHS had fully implemented one of our six recommendations (identifying staff roles and responsibilities) and had taken some action to implement the others. See GAO, *Information Technology: Management Improvements Needed on the Department of Homeland Security's Next Generation Information Sharing System*, GAO-09-40, (Washington, D.C.: Oct. 2008).

DHS's Information-Sharing Efforts Could be Enhanced by Developing More Specific Goals and Measures and Obtaining Additional Industry Feedback

DHS and TSA Have Established Goals and Measures Related to Information Sharing, but Their Goals Are Not Specific to Public Transit and Existing Measures May Limit Program Assessment

DHS and TSA have established goals and output-oriented performance measures for their information-sharing activities to help gauge the effectiveness of their overall information-sharing efforts with security stakeholders.[47] However, they have not developed performance goals and outcome-oriented measures to gauge the effectiveness of their information-sharing efforts specific to public transit agencies. Specifically, DHS and TSA have not developed such goals and measures for HSIN-PT and the PT-ISAC—mechanisms designed to serve as the primary information sources for the public transit agencies—or the recently established TS-ISAC. As a result, DHS and TSA may not be fully informed of the effectiveness of their information-sharing activities for the public transit industry. TSA officials recognize the importance of establishing specific goals and developing outcome-oriented measures, but they are in the beginning stages of doing so and could not provide time frames for when they plan to complete these efforts. Table 7, below, details DHS's current goals and performance measures related to information sharing.

[47] Performance measures can be classified as output, process/input, or outcome oriented. Output measures focus on the quantity of direct products and services a program delivers. Process/input measures address the type or level of program activity an organization conducts and the resources used by the program. Outcome measures offer information on the results of the direct products and services a program has delivered.

Table 7: DHS and TSA Performance Goals and Measures for Information-Sharing Activities

Agency	Goal	Measure	Focus	Source
DHS	Detect, deter, and prevent terrorist incidents by sharing domestic situational awareness through national operational communications and intelligence analysis.	(1) Number of Homeland Intelligence Reports disseminated[a]. (2) Percentage of breaking homeland security situations disseminated to designated partners within targeted time frames.	Homeland security stakeholders	*DHS Annual Performance Report Fiscal Years 2008-2010*
DHS	Provide, build, and support a robust information-sharing capability among and between federal and state, local, and tribal partners.	None	Homeland security stakeholders	I&A 2009 Strategy
TSA	Prevent or deter acts of terrorism using or against the transportation system.	None	Transportation industry, including mass transit	TSA Transportation Systems Sector Specific Plan and accompanying Mass Transit Modal Annex
TSA	Improve the timely and secure exchange of transportation security information.	None	Homeland security stakeholders	TSISP 2009 Update
TSA	Establish a framework enabling secure, multidirectional transportation security information between government and industry.	None	Homeland security stakeholders	TSISP 2009 Update

Source: GAO analysis of DHS and TSA information.

Note: "None" as used in the performance measures column refers to the lack of performance measures identified by DHS and TSA in writing or orally.

[a] Homeland Intelligence Reports provide emergent intelligence information to security stakeholders. The DHS *Annual Performance Report Fiscal Years 2007-2009* also measured the percentage of active HSIN users. However, this measure has been temporarily discontinued due to account verification process issues. This measure was not included in the *DHS Annual Performance Report Fiscal Years 2008-2010*.

The performance goals and measures established by DHS and TSA are primarily focused on information-sharing efforts with homeland security stakeholders and the transportation community as a whole, and are not specific to their efforts to share security-related information with the public transit industry.[48] TSA has developed some output-oriented

[48] As of July 2010, DHS I&A officials reported that they have updated their performance measures related to information sharing. However, I&A did not provide us with any additional details on these measures.

performance measures specifically for assessing its efforts to share security-related information with public transit agencies. According to TSA officials, the agency currently tracks: (1) the number of meetings held between the GCC and the Mass Transit SCC and the number of Transit Security and Safety Roundtables; (2) the number of teleconferences it conducts with the peer advisory group and the number of intelligence/information products it releases; and (3) the usage of the public transit subportal on HSIN as an indicator of stakeholders' interest in the information provided. TSA-OI is also collecting output data to measure the performance of the TS-ISAC, such as the number of users, the length of time each user is logged-on to the site, and the number of times users access information from the Web site.

We have previously reported that decision makers use performance measurement information, including output measures and information on program operations, to help identify problems in individual programs, identify causes of the problems, and modify services or processes to address problems.[49] However, leading management practices emphasize that successful performance measurement focuses on assessing the results of individual programs and activities.[50] We have also previously reported that without effective performance measurement, especially data on program outcomes, decision makers may have insufficient information to evaluate the cost-effectiveness of their activities.[51] While output measures, such as those developed by TSA, are useful because they indicate the quantity of direct services a program delivers, they do not reflect the overall effectiveness of their activities. 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

[49] GAO, *Aviation Security: A National Strategy and Other Actions Would Strengthen TSA's Efforts to Secure Commercial Airport Perimeters and Access Controls*, GAO-09-399 (Washington, D.C.: Sept. 2009).

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

[51] GAO, *Homeland Security: Guidance and Standards Are Needed for Measuring Effectiveness of Agencies' Facility Protection Efforts*, GAO-06-612 (Washington, D.C.: May 2006).

measures, but have called on agencies to take steps towards establishing such measures to hold them accountable for the investments they make. Furthermore, developing such measures provides agencies with valuable information for evaluating the effectiveness of their programs and the extent to which they are meeting their goals.

Furthermore, TSA has not developed specific performance goals or outcome-oriented measures for the PT-ISAC or HSIN-PT, which were both established as primary information-sharing mechanisms for public transit agencies. According to TSA and APTA officials, they plan to develop specific goals and measures for the PT-ISAC through the GCC/SCC Information Sharing Working Group. However, the working group is still finalizing its options for enhancing information-sharing efforts with public transit agencies, including assessing opportunities to streamline existing information-sharing mechanisms, and TSA officials were unable to provide us with time frames concerning the completion of these efforts.[52] In regard to HSIN-PT, TSA has developed an output-oriented performance measure which tracks the number of users of this mechanism; however, this measure provides limited information on which the agency can assess the results and progress of this information-sharing mechanism. TSA-OI, however, has not developed specific goals or outcome-oriented performance measures for HSIN-PT. Moreover, TSA-OI officials reported that for the newly established TS-ISAC, they are focusing on providing security-related products to 100 percent of homeland security stakeholders, including public transit agencies. However, TSA has not developed goals or related performance measures for this mechanism and could not provide time frames for doing so.[53] Once the SCC/GCC Information Sharing Working Group has developed options for improving information sharing with public transit agencies, establishing time frames for developing goals and related, outcome-oriented measures for the PT-ISAC, HSIN-PT, and TS-ISAC could assist TSA in obtaining more meaningful information from which to gauge the effectiveness of these information-sharing mechanisms.

[52] According to APTA officials, the Information Sharing Working Group has focused its current efforts on improving the PT-ISAC's transportation security products, and, to date, has not focused on developing a performance measurement system for this mechanism.

[53] TSA-OI officials stated that the focus of their information-sharing activities for the TS-ISAC is based on the information-sharing requirements in the 9/11 Commission Act.

DHS Has Taken Steps to Gather Feedback on Public Transit Agencies' Satisfaction with the Security-Related Information They Receive, but Has Not Established a Systematic Process for Collecting Such Information

DHS and TSA have taken some steps to gather feedback on public transit agencies' satisfaction with the security-related information they receive. For example, DHS and TSA developed forms to periodically gather feedback on security-related products from their customers, including public transit agencies. TSA officials also reported that they informally gather feedback during the Transit Security and Safety Roundtables. However, a systematic process for obtaining feedback on the usefulness of the PT-ISAC and HSIN-PT does not currently exist. We have previously reported that agencies with a systematic process for gathering feedback use surveys and other methods to identify the importance or depth of customers' issues in a single, centralized framework, and integrate the feedback information obtained in a standard and consistent manner.[54] In December 2009, we reported that additional DHS actions to obtain feedback on the utility and quality of information shared could strengthen the department's efforts in this area.[55] Research of best practices for customer satisfaction suggests that multiple approaches to customer feedback, such as focus groups and complaint programs that provide qualitative and quantitative data, and the integration of feedback data, are needed to effectively listen and understand customers' needs and to take appropriate action to meet those needs.[56]

In March 2010, DHS I&A began attaching a survey to each of its FOUO intelligence products that are disseminated to all its customers, including state and local partners, who receive FOUO products, to better understand customer information needs. Public transit agencies that receive I&A's FOUO intelligence products will therefore have an opportunity to provide feedback on the information provided. I&A officials stated that they plan to use these results to better inform them of product usefulness and the security information needs of their customers. In addition, TSA-OI posted a feedback form on the TS-ISAC to gather users' views, including public transit agencies, on TSA-OI products. However, TSA-OI's marketing materials on the TS-ISAC did not reference this feedback survey, nor has the agency informed users of this survey's existence through any other method. In addition, according to TSA-OI officials, this survey was posted shortly after the TS-ISAC was implemented in March 2010, but as of May

[54] GAO-02-776.

[55] GAO, *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. 2009).

[56] GAO-02-776.

27, 2010, TSA-OI had not received any feedback through this survey. Due to the recent timing of these survey efforts, it may be too early to assess the insights that will be provided through this mechanism.

Although TSA officials have established a process to gather user views, including public transit agencies, on TSA-OI products, TSA has not established a systematic process to obtain public transit agencies' feedback on information shared through the PT-ISAC and through HSIN-PT— the primary mechanisms designed to share security-related information with public transit agencies. Also, as of July 2010, TSA officials stated that they are uncertain about whether or not they will continue to use the TS-ISAC feedback form as a mechanism to gather public transit agency feedback. However, they stated that the agency does not have a systematic process in place to request, collect, and analyze feedback in order to gauge public transit agencies' overall satisfaction with its information-sharing activities, and that such a process is needed. TSA officials could consider using various survey tools and other methods to assist them in collecting public transit agency feedback, which could better inform them of the effectiveness of their information-sharing efforts. For example, through our survey, we were able to assess the extent to which these public transit agencies used and were satisfied with a variety of information-sharing mechanisms, including TSA mechanisms. DHS's and TSA's efforts to share security-related information with public transit agencies could be enhanced by developing a systematic process for gathering feedback on these agencies' satisfaction with the information they receive.

Conclusions

The recent bombings on the Moscow subway and planned attempts to detonate explosives in the New York City subway system have highlighted the continued threat to public transit systems in foreign countries and in the United States. While the SCC/GCC Information Sharing Working Group's efforts to enhance information sharing with public transit agencies reflects the joint stakeholder commitment to this area, opportunities for strengthening information sharing exist. Until TSA establishes time frames for the SCC/GCC Information Sharing Working Group to complete its efforts, including assessing opportunities to streamline existing information-sharing mechanisms and conducting targeted outreach efforts to increase awareness of the PT-ISAC and HSIN, the agency is limited in its ability to take further action to strengthen information sharing. In addition, without taking steps to ensure that the PT-ISAC fulfills its responsibilities and completes agreed-upon tasks, TSA and FTA cannot be assured that this mechanism meets the security

information needs of public transit agencies. Further, while DHS and TSA are taking steps to improve information sharing with public transit agencies, this effort will not be complete until the accessibility and user-friendliness of HSIN are addressed. Moreover, the HSIN-PT subportal will likely continue to be underutilized until DHS takes steps to ensure that this mechanism contains security-related information that is of value to public transit agencies.

Once the SCC/GCC Information Sharing Working Group develops options for improving information sharing with public transit agencies, it will be important for DHS and TSA to continue with other efforts to strengthen this area of information sharing. Specifically, until DHS establishes time frames for developing goals and related outcome-oriented performance measures for the PT-ISAC, HSIN-PT, and TS-ISAC, the department will be limited in its ability to gauge the effectiveness of its information-sharing efforts with the public transit industry. Finally, while we are encouraged by the department's efforts to gather feedback on public transit agencies' satisfaction with the security-related information they receive, a systematic process for obtaining such feedback on the PT-ISAC and HSIN-PT is lacking. Such a process could help DHS and TSA assess the effectiveness of their efforts to share security-related information with public transit agencies.

Recommendations for Executive Action

To help strengthen information sharing with public transit agencies, we recommend that the Secretary of Homeland Security direct the Assistant Secretary for the Transportation Security Administration to take the following action in coordination with FTA and public transit agencies:

- Establish time frames for the SCC/GCC Information Sharing Working Group to develop options for improving information sharing to public transit agencies and complete this effort, including the Working Group's efforts to:
  - assess opportunities to streamline existing information-sharing mechanisms that target similar user groups with similar information to reduce overlap, where appropriate; and
  - conduct targeted outreach efforts to increase awareness of the PT-ISAC and HSIN among agencies that are not currently using or aware of these systems.

To help ensure that the PT-ISAC is meeting its objectives for sharing security-related information with public transit agencies, we recommend that the Secretaries of Homeland Security and Transportation direct the Assistant Secretary of the Transportation Security Administration and

Administrator of the Federal Transit Administration to take the following action:

- Take steps to ensure the PT-ISAC fulfills its responsibilities and completes agreed-upon tasks.

To help strengthen DHS's efforts to share security-related information with public transit agencies, we recommend that the Secretary of Homeland Security take the following three actions:

- Take steps to ensure that public transit agencies can access and readily utilize HSIN and that the HSIN-PT subportal contains security-related information that is of value to public transit agencies.
- Once the SCC/GCC Information Sharing Working Group has developed options for improving information sharing with public transit agencies, establish time frames for developing goals and related outcome-oriented performance measures specific to the PT-ISAC, HSIN-PT, and TS-ISAC.
- Develop a process for systematically gathering feedback on public transit agencies' satisfaction with the PT-ISAC and HSIN-PT.

Agency Comments and Our Evaluation

We provided a draft of this report and its accompanying e-supplement (GAO-10-896SP) to DHS, DOJ, and DOT for review and comments. We received written comments from DHS on the draft report, which are summarized below and reproduced in full in appendix IV. DHS concurred with the report and recommendations and indicated that it is taking steps to address the recommendations. DHS also provided technical comments that we incorporated where appropriate. In an E-mail received September 7, 2010, the FBI liaison stated that the Bureau had no comments on the draft report. DOT did not provide comments on the findings and recommendations but did provide technical comments to the draft report, which we have incorporated where appropriate. DHS, DOJ, and DOT did not provide comments on the e-supplement.

In commenting on the draft report, DHS described the efforts the department has underway or planned to address our recommendations. These efforts are intended to improve information sharing with public transit agencies. However, although the actions DHS reported are important first steps, additional efforts are needed to help ensure that our recommendations are fully implemented, as discussed below.
With regard to our first recommendation that TSA coordinate with FTA and public transit agencies to establish time frames for the SCC/GCC

Information Sharing Working Group for completing efforts to develop options for improving information sharing to public transit agencies, including assessing opportunities for streamlining existing mechanisms and conducting targeted outreach, DHS stated that TSA is continuing to work with members of the working group to identify options on how to streamline the flow of information and described one such option. According to DHS, the working group has identified at least one product option for streamlining information sharing that would match the needs of stakeholders. This product would be "pushed" out to stakeholders and also be posted on appropriate websites. DHS also stated that TSA is taking steps to improve targeted outreach through collaboration of the Surface Transportation Information Sharing and Analysis Center and the PT-ISAC in the development of periodic intelligence summaries and plans to work with both ISACs, as well as DHS to ensure further outreach is conducted with stakeholders. TSA's efforts to streamline information sharing with public transit agencies and improve its outreach are important first steps toward improving the information provided to the public transit industry. In order to meet the full intent of our recommendation, TSA should establish time frames for completing these efforts. In addition, TSA did not indicate whether it has identified other options or is considering taking additional steps to streamline existing information sharing mechanisms or how its outreach to public transit agencies will be targeted to those agencies not currently using or aware of these systems. Taking such actions would be necessary to fully address the intent of this recommendation.

Regarding our second recommendation that TSA and FTA take steps to ensure the PT-ISAC fulfills its responsibilities and completes agreed-upon tasks, DHS stated that the purpose for including HSIN-PT content management and other elements currently in the cooperative agreement with APTA/PT-ISAC was to fill gaps in the information sharing process used by the mass transit and passenger rail community. DHS also stated that TSA intends to ensure compliance with the contract elements by "phasing in PT-ISAC contributions and requirements to achieve maximum effectiveness." TSA's stated plan for ensuring compliance with contract elements appears to be a positive step. However, DHS's response did not indicate the specific steps that will be taken to ensure that the PT-ISAC fulfills its responsibilities and completes agreed-upon tasks. Taking such action would more fully address our recommendation.

In regards to our third recommendation that DHS take steps to ensure that public transit agencies can access and readily utilize HSIN and that the HSIN-PT subportal contains security-related information that is of value to

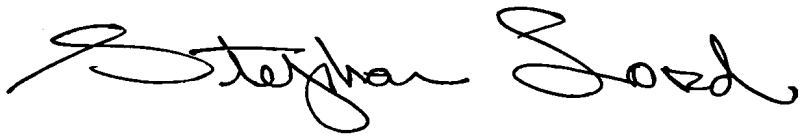
public transit agencies, DHS stated that it supports changes to HSIN and the intensification of efforts to expand its use for the broader range of transit and passenger rail agencies. DHS also stated that in fiscal year 2010, the HSIN program increased its efforts to raise the awareness of HSIN through a targeted marketing strategy. DHS also stated that the HSIN program's requirements management process and operator representation on the HSIN Mission Operators Committee governance board will ensure that public transit sector requirements are assessed, prioritized, and implemented. While DHS's reported efforts to expand HSIN use with the public transit community are noteworthy, in order to meet the full intent of our recommendation, DHS should also take steps to ensure that public transit agencies can readily access and use HSIN, as we recommended. Additionally, DHS did not clearly identify the actions it will take to ensure that the HSIN-PT subportal contains security-related information that is of value to public transit agencies. Identifying and implementing such steps would be necessary to fully address the intent of our recommendation.

With regard to our fourth recommendation that DHS establish time frames for developing goals and related outcome-oriented performance measures specific to the PT-ISAC, HSIN-PT, and TS-ISAC, DHS agreed that developing outcome-oriented measures for information sharing is important. Specifically, DHS stated that TSA will work with DHS, APTA, and the PT-ISAC to develop a series of goals and measures to assess the effectiveness of its information-sharing efforts. DHS added that these measures, once developed, can be expected to evolve and improve over time as systematic improvements are made. DHS plans to share the developed measures with its stakeholders to obtain their comments. In order to meet the full intent of our recommendation, DHS should establish time frames for developing such goals and measures.

Concerning our fifth recommendation that DHS develop a process for systematically gathering feedback on public transit agencies' satisfaction with the PT-ISAC and HSIN-PT, DHS stated that updates to HSIN will enable the department to efficiently capture user feedback. DHS also stated that it would need to collaborate with TSA and DOT as well as industry stakeholders to develop additional stakeholder feedback mechanisms. DHS also noted that is will continue to obtain stakeholder feedback through its survey on the TS-ISAC subportal. While the development of the customer survey on the TS-ISAC is an important step in obtaining feedback on the satisfaction of this mechanism, DHS should ensure that its process for gathering feedback on public transit agencies' satisfaction with the PT-ISAC and HSIN-PT is systematic, as we

recommended. Taking such action is necessary to fully address this recommendation.

We are sending copies of this report to the Secretaries of Homeland Security and Transportation, and the Attorney General. The report is also available at no charge on GAO's Web site at http://www.gao.gov. If you or your staff have any questions about this report, please contact me at (202) 512-4379 or lords@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix V.



Stephen M. Lord
Director, Homeland Security and Justice Issues

List of Committees

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

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

The Honorable James L. Oberstar
Chairman
The Honorable John L. Mica
Ranking Member
Committee on Transportation and Infrastructure
House of Representatives

Appendix I: Objectives, Scope, and Methodology

This report addresses the following questions: (1) What mechanisms has the federal government established or funded as primary information-sharing sources for public transit agencies? (2) To what extent are public transit agencies satisfied with federal efforts to share security-related information, and how, if at all, can these efforts be improved? (3) To what extent has the Department of Homeland Security (DHS) identified goals for sharing security-related information with public transit agencies and developed measures to gauge its progress in meeting those goals?

To identify the mechanisms established or funded by the federal government to serve as primary information sources for public transit agencies, we reviewed and assessed relevant documentation, such as the Homeland Security Information Network (HSIN) Program Management Plan, and interviewed officials from DHS components including the Office of Infrastructure Protection (IP) within the National Protection and Programs Directorate (NPPD), the Office of Intelligence and Analysis (I&A), the U.S. Coast Guard, and the Transportation Security Administration (TSA), as well as officials from the Federal Transit Administration (FTA) and the Federal Bureau of Investigation (FBI) to discuss the mechanisms they use to share security-related information with public transit agencies.[1] We also conducted site visits, or held teleconferences, with security and management officials from a nonprobability sample of 27 public transit agencies across the nation to determine which mechanisms are most routinely used by these agencies to obtain security-related information. These transit agencies were selected to generally reflect the variety of transit agencies in terms of size, location, transportation mode, and law enforcement presence and represent about 63 percent of the nation's total public transit ridership based on information we obtained from FTA's National Transit Database. Because we selected a nonprobability sample of transit agencies to interview, the information obtained cannot be generalized to the overall population of transit agencies. However, the interviews provided illustrative examples of the perspectives of various transit agencies about federal government information-sharing mechanisms and corroborated information we gathered through other means. Table 8 lists the public transit agencies we interviewed.

[1] We did not include Amtrak in the scope of this review because federal transportation law excludes Amtrak in its definition of public transportation. 49 U.S.C. § 5302.

Table 8: Public Transit Agencies Interviewed

Public transit agency	Urban area served[a]
Alameda-Contra Costra Transit District (AC Transit)	Oakland, California
Bay Area Rapid Transit	San Francisco, California
Chicago Transit Authority	Chicago, Illinois
Fairfax Connector Bus System	Fairfax, Virginia
City of Tempe Transportation Planning and Transit Division-Valley Metro	Phoenix-Mesa, Arizona
Greater Richmond Transit Company	Richmond, Virginia
Golden Gate Bridge, Highway and Transportation District	San Francisco, California
Gwinnett County Transit	Atlanta, Georgia
Long Beach Transit	Los Angeles-Long Beach-Santa Ana, California
Los Angeles County Metropolitan Transportation Authority	Los Angeles, California
Maryland Transit Administration	Baltimore, Maryland
Metropolitan Atlanta Rapid Transit Authority	Atlanta, Georgia
Metro-North Commuter Railroad Company	New York, New York-Newark, New Jersey-Connecticut
Metropolitan Transportation Authority Bus	New York, New York-Newark, New Jersey-Connecticut
Metropolitan Transportation Authority Long Island Railroad	New York, New York-Newark, New Jersey-Connecticut
Metropolitan Transportation Authority New York City Transit	New York, New York-Newark, New Jersey-Connecticut
Montgomery County Transit	Washington, D.C., Virginia, Maryland
New Jersey Transit	Newark, New Jersey-New York, New York
New York Department of Transportation-Staten Island Ferry	New York, New York-Newark, New Jersey-Connecticut
Northeast Illinois Regional Commuter Railroad Corporation-METRA	Chicago, Illinois-Indiana
Northern Indiana Commuter Transportation District	Chicago, Illinois-Indiana
Orange County Transportation Authority	Los Angeles-Long Beach-Santa Ana, California
Pace - Suburban Bus Division	Chicago, Illinois-Indiana
Port Authority Trans-Hudson Corporation-PATH	New York, New York- New Jersey
San Francisco Municipal Railway-MUNI	San Francisco-Oakland, California
Southern California Regional Rail Authority-Metrolink	Los Angeles-Long Beach-Santa Ana, California
Washington Metropolitan Area Transit Authority	Washington, D.C., Virginia, Maryland

Source: GAO

[a]The urban area served is consistent with the information contained in the National Transit Database.

To assess the satisfaction of public transit agencies with federal security-related information- sharing efforts and related opportunities for improvement, in March and April 2010, we surveyed 96 of the of the 694 U.S. public transit agencies as of 2008, by ridership statistics, on their

satisfaction with information-sharing efforts.[2] The 96 public transit agencies surveyed represent about 91 percent of total 2008 ridership. For the purposes of this survey, we defined the six aspects of quality security-related information as (1) relevance (i.e., is the information sufficiently relevant to be of value to a public transit agency?); (2) validity (i.e., is the information accurate?); (3) timeliness (i.e., is information received in a timely manner?); (4) completeness (i.e., does the information contain all the necessary details?); (5) actionability (i.e., would the information allow a public transit agency to change its security posture, if such a change was warranted?); and (6) access/ease of use (i.e., is information available through this mechanism easy to obtain?). To develop the survey instrument, we conducted pretest interviews with four public transit agencies and obtained input from GAO experts. Out of the original population of 96 transit agencies, we received completed questionnaires from 80 respondents—a response rate of 83 percent; however, not all respondents provided answers to every question.

The final instrument, reproduced in an e-supplement we are issuing concurrent with this report—GAO-10-896SP—displays the counts of responses received for each question. The questionnaire asked those public transit officials responsible for security operations to identify the modes of transportation they provide, the extent to which they house their own law enforcement component, the mechanisms they use to obtain security information, and their satisfaction with each of these mechanisms.

While we surveyed 96 agencies of the largest U.S. public transit agencies, and thus our data are not subject to sampling error, the practical difficulties of conducting any survey may introduce other errors in our findings. We took steps to minimize errors of measurement, nonresponse, and data processing. In addition to the questionnaire development and testing activities described above, we made multiple follow-up attempts by E-mail and telephone to reduce the level of nonresponse throughout the

[2] The total number of public transit agencies reflects those agencies that reported data to the National Transit Database in 2008. We surveyed 96 of the top 100 agencies as measured by fiscal year 2008 ridership. We omitted two agencies after learning these two entities are each comprised of multiple smaller transit agencies that, for ease of reporting, consolidate their annual ridership totals in the National Transit Database. In addition, we omitted two other agencies after learning that the security points-of-contact at these two agencies were also responsible for security at two other top-100 agencies and consequently already received our survey.

survey period. Finally, analysis programs and other data analyses were independently verified.

To further address this question, we assessed relevant documentation, including interagency agreements between TSA and FTA, as well as marketing materials on the Transportation Security Information Sharing and Analysis Center (TS-ISAC). We also interviewed American Public Transportation Association (APTA), Public Transportation Information Sharing and Analysis Center (PT-ISAC), TSA, FBI, FTA, and DHS Operations, Coordination, and Planning Directorate officials to discuss efforts to streamline existing information-sharing mechanisms, oversee the results of the PT-ISAC, and conduct outreach on various information-sharing mechanisms. We compared these efforts to internal control standards, as well as our previous work on the need to consolidate redundant information systems and target outreach efforts. In addition, we interviewed select public transit agencies and included questions in our Web-based survey of public transit agencies on the various information-sharing mechanisms available to them.

To assess the extent to which DHS has identified goals for sharing information with public transit agencies and developed measures to gauge its progress in meeting those goals, we reviewed DHS's Annual Performance Report, TSA's Transportation Security Information Sharing Plan (TSISP), and available performance data and measures for fiscal years 2007 through 2010 related to information-sharing efforts with public transit agencies and compared them to leading management practices and our previous work on program assessments. We also interviewed relevant DHS and TSA officials to obtain information on their efforts to revise and develop performance measures and goals for this area of information sharing, as well as their efforts to obtain feedback from public transit agencies on their satisfaction with the security-related information they receive. In addition, we compared TSA's efforts to evaluate their information-sharing efforts with guidance on performance measurement contained in our previous reports.

We conducted this performance audit from August 2009 through September 2010 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: National Strategies, Plans, and Reports Designed to Enhance Information Sharing

Since the terrorist attacks on September 11, 2001, the federal government has developed strategies to enhance the sharing of terrorism-related information among federal, state, local, and tribal agencies, and the private sector. These strategies include the following:

- *National Strategy for Information Sharing*: Issued in October 2007, this strategy identifies the federal government's information sharing responsibilities. These responsibilities include gathering and documenting the information that state, local, and tribal agencies need to enhance their situational awareness of terrorist threats. The strategy also calls for authorities at all levels of government to work together to obtain a common understanding of the information needed to prevent, deter, and respond to terrorist attacks. Specifically, the strategy discusses the need to improve the two-way sharing of terrorism-related information on incidents, threats, consequences, and vulnerabilities, including enhancing the quantity and quality of specific, timely, and actionable information provided by the federal government to critical infrastructure sectors.[1]

- *DHS Information Sharing Strategy*: Issued in April 2008, this strategy describes the guiding principles for DHS's efforts to share information within the department, across the federal government, and with state, local, tribal, territorial, private sector, and international partners. Among other things, the strategy notes that DHS must take steps to ensure that the right information gets to the right people at the right time. The strategy also discusses the department's need to institute performance measures to provide an accurate assessment of the department's progress towards meeting its information-sharing goals.

- *The National Infrastructure Protection Plan* (NIPP): Updated in 2009, the NIPP is intended to provide the framework for a coordinated national approach to address the full range of physical, cyber, and human threats and vulnerabilities that pose risks to the nation's critical infrastructure.[2] Among other things, the NIPP names TSA as the primary federal agency responsible for coordinating critical infrastructure protection efforts within the transportation sector and emphasizes the importance and

[1] There are 18 critical infrastructure sectors, including Agriculture and Food; Banking and Finance; Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Government Facilities; Information Technology; National Monuments and Icons; Nuclear Reactors, Materials and Waste; Postal and Shipping; Public Health and Healthcare; Transportation Systems; and Water.

[2] The first version of the NIPP was issued in June 2006.

benefits of sharing security-related information with critical sector partners.

- *Transportation Security Information Sharing Plan* (TSISP): Established by TSA in July 2008 pursuant to the 9/11 Commission Act and subsequently updated in December 2009.[3] The stated purpose of the TSISP is to establish a foundation for sharing transportation security information between all entities that have a stake in protecting the nation's transportation system, including federal, state, local, and tribal agencies and governments, the private sector, and foreign partners.

- *Surface Transportation Security Priority Assessment*: Issued in March 2010 by the Administration's Transborder Security Interagency Policy Committee, Surface Transportation Subcommittee. The study identified 10 issue areas to examine, obtained input from surface transportation sector stakeholders, and analyzed the responses to reach a consensus set of priorities and recommendations related to surface transportation. Among other things, the assessment included a recommendation that that TSA collaborate with DHS and the Department of Transportation (DOT) to more effectively share transportation security information.

[3] The TSISP was established in accordance with section 1203 of the 9/11 Commission Act. Pub. L. No. 110-53, § 1203(a), 121 Stat. 266, 383-85 (2007). According to the Transportation Security Administration Office of Intelligence (TSA-OI), the TSISP will be updated again by October 2010.

Appendix III: Public Transit Agencies' General Satisfaction with the 12 Most Frequently-Cited Information-Sharing Mechanisms

The table below illustrates, for the public transit agencies we surveyed, the general satisfaction along 6 quality dimensions with the 12 most frequently-cited information-sharing mechanisms.[1] The quality dimensions rated for level of satisfaction were: relevance (i.e., is the information sufficiently relevant to be of value to a public transit agency?); validity (i.e., is the information accurate?); timeliness (i.e., is information received in a timely manner?); completeness (i.e., does the information contain all the necessary details?); actionability (i.e., would the information allow a public transit agency to change its security posture, if such a change was warranted?); and access/ease of use (i.e., is information available through this mechanism easy to obtain?). The numbers in parentheses below each mechanism represent the number of agencies in our survey that indicated they use this mechanism to receive security-related information. For each mechanism and quality dimension, the table indicates (1) the number of agencies that indicated they were either "very satisfied" or "somewhat satisfied" with the information they receive through the mechanism (or, in the case of "access / ease of use," the mechanism itself); (2) the total number of agencies that provided a response to the question; and (3) the percentage of responding agencies that were generally satisfied. The mechanisms are organized in the order they were presented in the survey.

[1] We use the term generally satisfied to describe agencies that indicated they were either "very satisfied" or "somewhat satisfied" with the information they receive. Similarly, we use the term generally dissatisfied to describe agencies that indicated they were either "very dissatisfied" or "somewhat dissatisfied" with the information they receive.

Table 9: Public Transit Agencies' Survey Responses Regarding Satisfaction with 12 Information-Sharing Mechanisms Along 6 Dimensions of Quality

Mechanism (number of agencies that use mechanism)	Number and percentage of public transit agencies indicating general satisfaction along 6 quality dimensions[a]						
	Relevance	Validity	Timeliness	Completeness	Actionability	Access / ease of use	Overall general satisfaction
PT-ISAC (49)	37/49 *(76%)*	40/49 *(82%)*	36/49 *(73%)*	35/49 *(71%)*	30/49 *(61%)*	38/49 *(78%)*	**37/49** ***(76%)***
HSIN (34)[b]	19/34 *(56%)*	19/34 *(56%)*	18/33 *(55%)*	15/34 *(44%)*	15/34 *(44%)*	16/34 *(47%)*	**19/33** ***(58%)***
JTTF (53)	38/45 *(84%)*	34/45 *(76%)*	32/45 *(71%)*	34/45 *(76%)*	30/44 *(68%)*	34/45 *(76%)*	**34/44** ***(77%)***
Fusion Centers (39)	30/34 *(88%)*	29/34 *(85%)*	27/34 *(79%)*	26/34 *(76%)*	23/34 *(68%)*	26/33 *(79%)*	**27/34** ***(79%)***
Transportation Security Operations Center (TSOC) (41)	27/36 *(75%)*	26/36 *(72%)*	21/36 *(58%)*	21/36 *(58%)*	22/35 *(63%)*	23/36 *(64%)*	**22/36** ***(61%)***
Transit Security & Safety Roundtables (44)	32/36 *(89%)*	32/36 *(89%)*	28/36 *(78%)*	29/35 *(83%)*	28/36 *(78%)*	31/35 *(89%)*	**33/36** ***(92%)***
Other public transit systems (48)	31/35 *(89%)*	31/35 *(89%)*	26/35 *(74%)*	27/35 *(77%)*	28/33 *(85%)*	26/34 *(76%)*	**28/35** ***(80%)***
FTA E-mails (65)	47/53 *(89%)*	48/53 *(91%)*	44/50 *(88%)*	45/52 *(87%)*	42/53 *(79%)*	44/52 *(85%)*	**42/51** ***(82%)***
TSA E-mails (56)	41/46 *(89%)*	40/45 *(89%)*	39/45 *(87%)*	38/44 *(86%)*	39/46 *(85%)*	38/45 *(84%)*	**38/46** ***(83%)***
Industry association (e.g., APTA) (44)	23/30 *(77%)*	23/30 *(77%)*	19/30 *(63%)*	22/30 *(73%)*	16/30 *(53%)*	21/30 *(70%)*	**21/30** ***(70%)***
Regional information sharing mechanism (47)	28/34 *(82%)*	29/34 *(85%)*	27/33 *(82%)*	28/34 *(82%)*	24/34 *(71%)*	30/34 *(88%)*	**27/34** ***(79%)***
Regional emergency operations center (38)	25/28 *(89%)*	25/27 *(93%)*	26/28 *(93%)*	21/27 *(78%)*	20/28 *(71%)*	23/28 *(82%)*	**22/28** ***(79%)***

Source: GAO analysis of survey results.

[a] We use the term generally satisfied to describe agencies that indicated they were either "very satisfied" or "somewhat satisfied" with the information they receive. Similarly, we use the term generally dissatisfied to describe agencies that indicated they were either "very dissatisfied" or "somewhat dissatisfied" with the information they receive.

[b] For HSIN, the number in parentheses represents the 34 agencies that indicated they had log-in access to HSIN and had not lost or forgotten their password. Of these 34 agencies, 17 indicated they access the system less than once a month to obtain security-related information.

Appendix IV: Comments from the Department of Homeland Security

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

Homeland Security

September 15, 2010

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

Dear Mr. Lord:

RE: Response to Draft Report GAO-10-895, *Public Security Information Sharing: DHS Could Improve Information Sharing Through Streamlining and Increased Outreach*

Thank you for the opportunity to review and comment on the Government Accountability Office's (GAO) draft report referenced above (Job Code 440815). The Department of Homeland Security (DHS) concurs with the five recommendations in the draft report.

DHS and the Transportation Security Administration (TSA) value GAO's comprehensive review of efforts in addressing transit and passenger rail security, and we intend to immediately implement its recommendations. We appreciate the professionalism demonstrated by GAO's team members in conducting this review.

TSA and DHS also appreciate GAO's finding that our stakeholders are generally satisfied with the existing information sharing efforts. The Implementing Recommendations of the 9/11 Commission Act of 2007 highlighted the importance of improving information sharing efforts and provided additional tools to achieve this. TSA funding for the Public Transportation Information Sharing and Analysis Center (PT-ISAC) will allow for broader use of the ISAC in this effort and will provide the Sector Coordinating Council (SCC)/Government Coordinating Council (GCC) Information Sharing Working Group an opportunity to shape a more effective program and outcome-oriented metrics.

The progress of the existing information sharing program to date has been achieved through effective public-private partnerships in the mass transit and passenger rail mode and TSA's close coordination with other Federal agencies, particularly the Department of Transportation/Federal Transit Authority and the Department of Homeland Security – Infrastructure Protection. The Mass Transit SCC has also played a significant role in strengthening information sharing, and we believe the SCC will continue its efforts. The combined efforts of these organizations will produce an enhanced information sharing program. TSA looks forward to implementing plans developed with its partners to further integrate intelligence information and to conduct operational pilots of a daily intelligence summary.

We offer the following responses to the recommendations:

Recommendation 1: To help strengthen information sharing with public transit agencies, GAO recommends that the Secretary of Homeland Security direct the Assistant Secretary for the Transportation Security Administration in coordination with FTA and public transit agencies establish timeframes for the GCC/SCC Information Sharing Working Group to develop options for improving information sharing to public transit agencies and complete this effort, including the Working Group's efforts to:

- **Assess opportunities to streamline existing information sharing mechanisms that target similar user groups with similar information to reduce overlap, where appropriate; and**
- **Conduct targeted outreach efforts to increase awareness of the PT-ISAC and HSIN among agencies that are not currently using or aware of these systems.**

Response: DHS concurs with this recommendation.

TSA continues to work with members of the Information Sharing Working Group to identify options on how best to streamline information flow. The working group has identified at least one operating model that appears to match the needs of both the stakeholders and those who produce these products. This particular model would "push out" periodic two page summaries to the stakeholders and also post them on appropriate websites. A library would house the principle documents from which the summaries are taken.

TSA is currently taking steps to improve targeted outreach through collaboration of the Surface Transportation ISAC (ST-ISAC) and the PT-ISAC in the development of periodic intelligence summaries. ST-ISAC information on the freight rail community's threat posture will be provided to both the mass transit and passenger rail communities through these intelligence summaries. As passenger trains run on freight rail tracks, this represents a significant security information sharing expansion.

TSA will work with both ISACs as well as with DHS to ensure further outreach is conducted to these stakeholder communities and that additional capabilities are approved and incorporated into the Homeland Security Information Network (HSIN) portal. TSA Mass Transit and Passenger Rail Division will also designate a specific point of contact to oversee this activity.

In the end, it is the stakeholders who will determine which information system fits their needs. Therefore, it is incumbent upon the government entities to stay connected to the stakeholders and their concerns. The Transit Policing and Security Peer Advisory Group (PAG) and the Mass Transit and Passenger Rail GCC/SCC components of the mode will play critical roles in this effort.

Recommendation 2: To help ensure that the PT-ISAC is meeting its objectives for sharing security-related information with public transit agencies, GAO recommends that the Secretaries of Homeland Security and Transportation direct the Assistant

Secretary of Transportation Security Administration and Administrator of the Federal Transit Administration to take the following action:

- **Take steps to ensure the PT-ISAC fulfills its responsibilities and completes agreed-upon responsibilities and tasks.**

Response: DHS concurs with this recommendation.

The purpose for including HSIN-PT content management and the other elements currently in the contract with APTA/PT-ISAC was to fill gaps in the information sharing process used by the mass transit and passenger rail community. TSA's intention in doing this was to use all the tools available to establish an effective information sharing regime and organize the flow of information in such a way as to maximize the overall efficiency.TSA intends to ensure compliance with the contract elements by phasing in PT-ISAC contributions and requirements to achieve maximum effectiveness. Our goal is to maximize the PT-ISAC's role in information sharing and make them an integral part of this program. The elements contained in the PT-ISAC contract were designed to support this development and long-term vision.

Recommendation 3: To help strengthen DHS's efforts to share security-related information with public transit agencies, GAO recommends that the Secretary of Homeland Security take the following action:

- **Take steps to ensure that public transit agencies can access and readily utilize HSIN and that the HSIN-PT sub-portal contains security-related information that is of value to public transit agencies.**

Response: DHS concurs with this recommendation.

The HSIN website contains important information for all critical sectors. An effective, easy to use, well populated HSIN-PT sub portal enhances the amount of critical information that is shared (and can be shared) with the transit and passenger rail stakeholder community. We support changes to the HSIN website and intensification of efforts to expand use of this important Government site for the broader range of transit and passenger rail agencies. In Fiscal Year 2010, the HSIN Program increased Outreach efforts five-fold to raise the awareness of HSIN through a targeted marketing strategy. The Outreach Team implemented a HSIN State and Local Mission Integration program by placing team members in key regional locations throughout the country and arranging speaking engagements for key HSIN leadership members at national and regional conferences.

The HSIN Program's refined requirements management process and operator representation on the HSIN Mission Operators Committee (MOC) governance board will ensure that Public Transit Sector requirements are assessed, prioritized, and implemented.

Stakeholders provided generally positive responses regarding overall information sharing in the mass transit and passenger rail area, and DHS and TSA support further improvements to inform public transit agencies regarding the threats that exist and mitigation measures to take to protect the traveling public.

3

According to the DHS Office of Infrastructure Protection, July 2010 HSIN-CS User Statistics data sheet, Mass Transit and Passenger Rail is one of the most active users of HSIN among the transportation modes and that use appears to be expanding.

Recommendation 4: To help strengthen DHS's efforts to share security-related information with public transit agencies, GAO recommends that the Secretary of Homeland Security take the following action:

- **Once the SCC/GCC Information Sharing Working Group has developed options for improving information sharing with public transit agencies, establish timeframe for developing goals and related outcome-oriented measures specific to the PT-ISAC, HSIN-PT, and TS-ISAC.**

Response: DHS concurs with this recommendation.

Developing outcome-oriented metrics for information sharing is an important element in establishing a program that has continuous improvement as one of its goals. TSA will work with DHS, APTA and the PT-ISAC to develop a series of goals and measures to assess effectiveness. Such metrics can be expected to evolve and improve over time as systematic improvements are made. Feedback will be an important part of this effort. Updates to the HSIN platform will enable DHS to efficiently capture usage measures.

Once we have developed a set of measures, we will share them with our stakeholder groups such as the PAG and the Mass Transit SCC to obtain their comments.

Recommendation 5: To help strengthen DHS's efforts to share security-related information with public transit agencies, GAO recommends that the Secretary of Homeland Security take the following action:

- **Develop a process for systematically gathering feedback on public transit agencies' satisfaction with the PT-ISAC and HSIN-PT.**

Response: DHS concurs with this recommendation.

The TS-ISAC currently includes a survey on the materials posted and distributed. This survey will continue to be used with the stakeholders. The Mass Transit and Passenger Rail Security Awareness Messages also contain information about HSIN-PT access and will incorporate a feedback mechanism similar to that of the TS-ISACs.

Designing additional stakeholder feedback mechanisms will require collaboration between TSA, DHS, and DOT as well as with the transit industry stakeholders. The positive stakeholder feedback provided by GAO for this report has set a standard that we will strive to continue. TSA will do its part in ensuring stakeholder feedback mechanisms are in place to collect the important thoughts and comments of those we serve. Updates to the HSIN platform will enable DHS to efficiently capture user feedback.

4

Once again, thank you for the opportunity to comment on this draft report. We look forward to working with you on future homeland security issues.

Sincerely,

Jerald E. Levine

Jerald E. Levine
Director
Departmental GAO/OIG Liaison Office

5

Appendix V: GAO Contact and Staff Acknowledgments

GAO Contact

Stephen M. Lord, (202) 512-4379

Acknowledgments

In addition to the contact named above, Jessica Lucas-Judy, Assistant Director, managed this assignment. Vanessa Dillard, Jeff C. Jensen, Nancy Meyer, Octavia Parks, and Meg Ullengren made significant contributions to the work. Tracey King provided significant legal support and analysis. Stanley J. Kostyla assisted with design and methodology. Carl Ramirez and Joanna Chan assisted with the survey design, implementation, and data analysis. Christopher Currie, Lara Miklozek, and Debbie Sebastian provided assistance in report preparation. Tina Cheng and Robert Robinson developed the report graphic.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Congressional Relations

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

Public Affairs

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