United States General Accounting Office

GAO

Report to the Committee on Appropriations, House of Representatives

May 2003

TRANSPORTATION SECURITY RESEARCH

Coordination Needed in Selecting and Implementing Infrastructure Vulnerability Assessments

GAO
Accountability•Integrity•Reliability

Highlights

Highlights of GAO-03-502, a report to the House Committee on Appropriations

Why GAO Did This Study

The events of September 11, 2001, increased attention on efforts to assess the vulnerabilities of the nation's transportation infrastructure and develop needed improvements in security. The Department of Transportation's (DOT) Research and Special Programs Administration (RSPA) had already begun research in this area in June 2001. The goals of RSPA's Transportation Infrastructure Assurance program are to identify, and develop ways to mitigate the impact of, threats to the nation's transportation infrastructure. DOT's Office of Intelligence and Security is responsible for defining the requirements for transportation infrastructure protection, ensuring that vulnerability assessments of transportation infrastructure are conducted, and taking action to mitigate those vulnerabilities.

The House Committee on Appropriations asked GAO to determine (1) the status and anticipated results of the Transportation Infrastructure Assurance (TIA) program, and (2) the extent to which RSPA and the Office of Intelligence and Security have coordinated their activities in selecting the vulnerabilities to be assessed and implementing the vulnerability assessments for the program. DOT and RSPA officials reviewed a draft of the report, agreed with its contents, and provided technical clarifications that we incorporated.

www.gao.gov/cgi-bin/getrpt?GAO-03-502.

To view the full report, including the scope and methodology, click on the link above. For more information, contact Katherine Siggerud at (202) 512-2834 or siggerudk@gao.gov.
.

May 2003

TRANSPORTATION SECURITY RESEARCH

Coordination Needed in Selecting and Implementing Infrastructure Vulnerability Assessments

What GAO Found

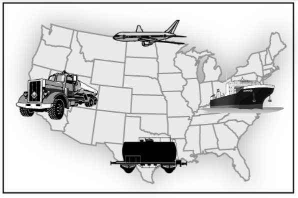
The Transportation Infrastructure Assessment program is scheduled to end in December 2003 after the completion of four transportation vulnerability assessments. Congress appropriated $1 million in each of the fiscal years from 2001 through 2003 to RSPA for the program. RSPA plans to disseminate reports, conduct workshops, and post information on the Internet to inform decision-makers in the transportation community about the results.

Program Vulnerability Assessments

Interdependency of the transportation system with other critical infrastructures: scheduled to be completed in May 2003; funding allocated - $1,000,000.

Feasibility of alternative backup systems for the global positioning system: scheduled to be completed in December 2003; funding allocated - $800,000.

Transportation and logistical requirements for emergency response teams in dealing with weapons of mass destruction: scheduled to be completed in May 2003; funding allocated - $600,000.



Options to transition hazardous materials transportation security guidelines to security requirements: scheduled to be completed in December 2003; funding allocated - $600,000.

Sources: FAA, Lockheed Martin Missiles & Space, OMB, and Nova Development Corporation.

Prior to March 2003, RSPA did not fully coordinate their activities with the Office of Intelligence and Security in selecting the vulnerabilities to be assessed, or in implementing the assessments for the program. We discussed this problem with officials from both offices who agreed that closer coordination would be beneficial, particularly to discuss options for addressing the challenges facing program researchers in conducting the program's vulnerability assessments. In March 2003, officials from both offices began regular meetings to facilitate this coordination.

Contents

Table

Figures

Abbreviations

DOT	Department of Transportation
FAA	Federal Aviation Administration
OIS	Office of Intelligence and Security
OMB	Office of Management and Budget
PDD	Presidential Decision Directive
RSPA	Research and Special Programs Administration
TIA	Transportation Infrastructure Assurance
TSA	Transportation Security Administration

G A O
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

May 1, 2003

The Honorable C. W. Bill Young
Chairman
The Honorable David R. Obey
Ranking Minority Member
Committee on Appropriations
House of Representatives

The terrorist attacks on the United States on September 11, 2001, increased attention on federal efforts to assess the vulnerabilities of the nation's transportation infrastructure and develop needed improvements in security. The Department of Transportation (DOT) formally began one such effort in June 2001—the Transportation Infrastructure Assurance program—within its Research and Special Programs Administration (RSPA). The Transportation Infrastructure Assurance program focuses on identifying and mitigating against threats, such as from acts of terrorism and sabotage, which could adversely affect the operation of the nation's transportation infrastructure and cause harm to humans. The program is crosscutting, defining "transportation infrastructure" to include highways, transit systems, railroads, airports, waterways, pipelines and ports, as well as the vehicles, aircraft, and vessels that operate on these networks. The program is also directly related to the mission of DOT's key transportation security stakeholder. DOT's Office of Intelligence and Security is responsible on behalf of the Secretary for defining the requirements for transportation infrastructure protection, ensuring that vulnerability assessments of transportation infrastructure are conducted, and taking action to mitigate those vulnerabilities.

In House Report 107-722, accompanying DOT and Related Agencies Appropriations Bill for fiscal year 2003, the House Appropriations Committee asked us to examine the Transportation Infrastructure Assurance program. In subsequent discussions with Committee staff we agreed to address the following questions: (1) What is the status and what are the anticipated results of the Transportation Infrastructure Assurance program? and (2) To what extent has RSPA coordinated their activities with DOT's Office of Intelligence and Security in selecting the vulnerabilities to be assessed and implementing the assessments for the program?

To answer these questions, we examined Transportation Infrastructure Assurance program documents, including budget data and project plans.

We also interviewed officials from RSPA's Office of Innovation, Research and Education—which manages the program, and the Volpe National Transportation Systems Center—which is conducting the program research—regarding the status, management, and operation of the program, as well as plans for disseminating and evaluating program results. In addition, we interviewed officials from the Office of Intelligence and Security about the extent of their participation in the program.

Although the Transportation Security Administration was formally part of DOT during the course of our review, it was not established until after the Transportation Infrastructure Assurance program began. Moreover, the Transportation Security Administration's initial efforts focused on safeguarding the nation's aviation industry; as a result, the Office of Intelligence and Security continued to lead DOT's efforts in fulfilling national critical infrastructure protection responsibilities. Consequently, our review focused on the Office of Intelligence and Security's involvement in the program. We did, however, talk with officials from the Transportation Security Administration regarding their role in identifying and undertaking future research activities necessary to enhance transportation security.

We conducted our review from September 2002 through February 2003 in accordance with generally accepted government auditing standards.

Results in Brief

The Transportation Infrastructure Assurance program is scheduled to end in December 2003 after completing four vulnerability assessments aimed at identifying and finding ways to mitigate threats against the nation's transportation infrastructure. RSPA's research center, the Volpe National Transportation System Center, in Cambridge, Massachusetts, is conducting the assessments to (1) examine the interdependency of the nation's transportation system with other critical infrastructures, such as energy and telecommunications; (2) identify the transportation and logistical requirements for emergency response teams in dealing with weapons of mass destruction; (3) examine the feasibility of alternative backup systems for the global positioning system, upon which aviation, maritime, and surface transportation industries rely; and (4) assess the options to transition from hazardous materials transportation security guidelines to security requirements. According to RSPA officials, RSPA plans to work with the Office of Intelligence and Security to disseminate program results to decision-makers in the transportation community through published reports, workshops, and the Internet. Congress appropriated $1 million in each of the fiscal years from 2001 through 2003 to RSPA for the Transportation Infrastructure Assurance program.

Prior to March 2003, RSPA did not fully coordinate their activities with the Office of Intelligence and Security in selecting the vulnerabilities to assess, or in implementing the assessments for the Transportation Infrastructure Assurance program. RSPA coordinated with the Office of Intelligence and Security in selecting two vulnerability assessments in fiscal year 2001. However, RSPA selected two additional transportation vulnerabilities for assessment in fiscal year 2002 without coordinating with the Office of Intelligence and Security. According to officials from RSPA and the Office of Intelligence and Security, this lack of coordination resulted in part from disagreements and misunderstandings about each other's respective role in the program. RSPA's coordination with the Office of Intelligence and Security during the research program's implementation has been limited to only one of the four vulnerability assessments under review. Greater coordination might have enabled officials from the Office of Intelligence and Security to obtain industry-sensitive information for RSPA's assessments and possibly increased the program's value, according to the Office of Intelligence and Security's Associate Director. During the course of our review, officials from both offices agreed with us that closer coordination would be beneficial to the program and agreed to meet regularly. We verified that in March 2003 officials from RSPA and the Office of Intelligence and Security began to meet regularly to facilitate this coordination. As a result, this report is making no recommendations. We provided a copy of the draft report to DOT and RSPA officials who agreed with the contents of the report and provided technical clarifications that we incorporated into the report.

Background

On May 22, 1998, President Clinton issued a pair of directives to guide federal efforts to address critical infrastructure vulnerabilities. Presidential Decision Directive 62 (PDD 62) highlighted the growing threat of unconventional attacks against the United States. It described a new and more systematic approach to fighting terrorism through interagency efforts to prepare for response to incidents involving weapons of mass destruction. Presidential Decision Directive 63 (PDD 63) further directed federal agencies to conduct risk assessments and planning efforts to reduce exposure to attack. Specifically, the assessments were to consider attacks that could significantly diminish the abilities of (1) the federal government to perform essential national security missions and ensure the general public health and safety; (2) state and local governments to maintain order and to deliver minimum essential public services; and (3) the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial, and transportation services. PDD 63 called for the government to complete these assessment efforts no later than May 2003. According to the Office of Intelligence and Security's (OIS) Associate Director for National Security (hereafter referred to as the Associate Director), the Transportation Infrastructure Assurance (TIA) program is, in part, DOT's effort to meet these Presidential Decision Directive requirements.

RSPA concentrates on multimodal issues (research that applies to more than one mode of transportation) that affect the entire U.S. transportation system rather than on a specific sector of the system. RSPA's Office of Innovation, Research and Education is responsible for managing the TIA program. The Volpe National Transportation Systems Center, located in Cambridge, Massachusetts, is the research arm of RSPA and is conducting the program's vulnerability assessments. OIS is the key transportation security stakeholder within DOT responsible for analyzing, developing, and coordinating departmental and national policies addressing national defense, border security, and transportation infrastructure assurance and protection issues. Other OIS responsibilities include: coordinating with the public and private sectors, international organizations, academia, and interest groups regarding issues of infrastructure protection; acting as the Secretary of Transportation's liaison with the intelligence, law enforcement, and national defense communities and assisting departmental organizations in establishing and maintaining direct ties with those communities; and serving as the Secretary of Transportation's primary advisor on significant intelligence issues affecting the traveling public, the transportation industry, and national security. According to OIS's Associate Director, OIS has historically been involved in the department's transportation security research efforts. He added that OIS's lead role in fulfilling the department's critical infrastructure responsibilities, including the implementation of Presidential Decision Directives addressing critical infrastructure vulnerabilities, is likely to change as the roles and responsibilities of the Transportation Security Administration (TSA) and the newly created Department of Homeland Security are defined.

Congress established TSA in November 2001[1] to be responsible for ensuring transportation security, including identifying and undertaking

[1] Aviation and Transportation Security Act, Public Law 107-71, 115 Stat. 597, Nov. 19, 2001.

research and development activities necessary to enhance transportation security. For fiscal year 2003, TSA received $110 million to fund transportation security research activities for all modes of transportation. Further, on November 25, 2002, the President signed the Homeland Security Act of 2002,[2] which established the Department of Homeland Security with the responsibility of, among other tasks, coordinating efforts in securing America's critical infrastructure. On March 1, 2003, TSA became part of the newly created Department of Homeland Security.

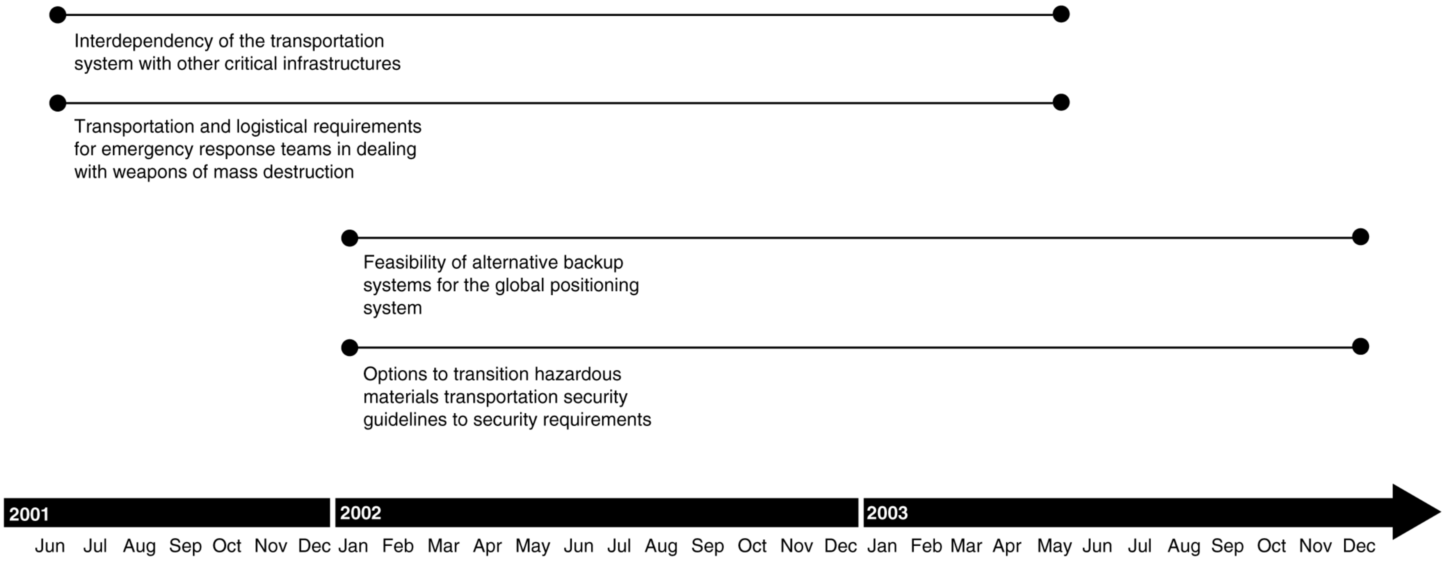
TIA Program Is Scheduled to End in December 2003 with Completion of Four Vulnerability Assessments

The TIA program is scheduled to end in December 2003, resulting in the completion of four vulnerability assessments aimed at identifying and finding ways to mitigate threats against the nation's transportation infrastructure. RSPA officials said that two of these assessments (the interdependency of the transportation system with other critical infrastructures and transportation and logistical requirements for emergency response teams in dealing with weapons of mass destruction) were selected, in part, to meet DOT's PDD 62 and 63 requirements, and are scheduled for completion in mid-2003 to meet the deadlines outlined in the presidential directives. The other two assessments (the feasibility of alternative backup systems for the global positioning system, and an assessment of the options to transition from hazardous materials transportation security guidelines to security requirements) were selected based upon a perceived need for assessments in these areas as defined by officials from RSPA's Office of Hazardous Materials Safety and the Volpe National Transportation Systems Center, and are scheduled for completion in December 2003. RSPA's Volpe Center is conducting the TIA program's four assessments and has conducted research related to transportation infrastructure since 1996. (See app. I for a summary of the Volpe Center's Workshops and Studies related to transportation infrastructure assurance from fiscal years 1996 to 2000.)

Figure 1 shows the TIA program's beginning and completion dates by specific vulnerability assessment. RSPA officials told us that it has no plans to include any additional or future assessments under the TIA program.

[2] Homeland Security Act of 2002, Public Law 107-296, 116 Stat. 2135, Nov. 25, 2002.

Figure 1: Beginning and Completion Dates of Vulnerability Assessments

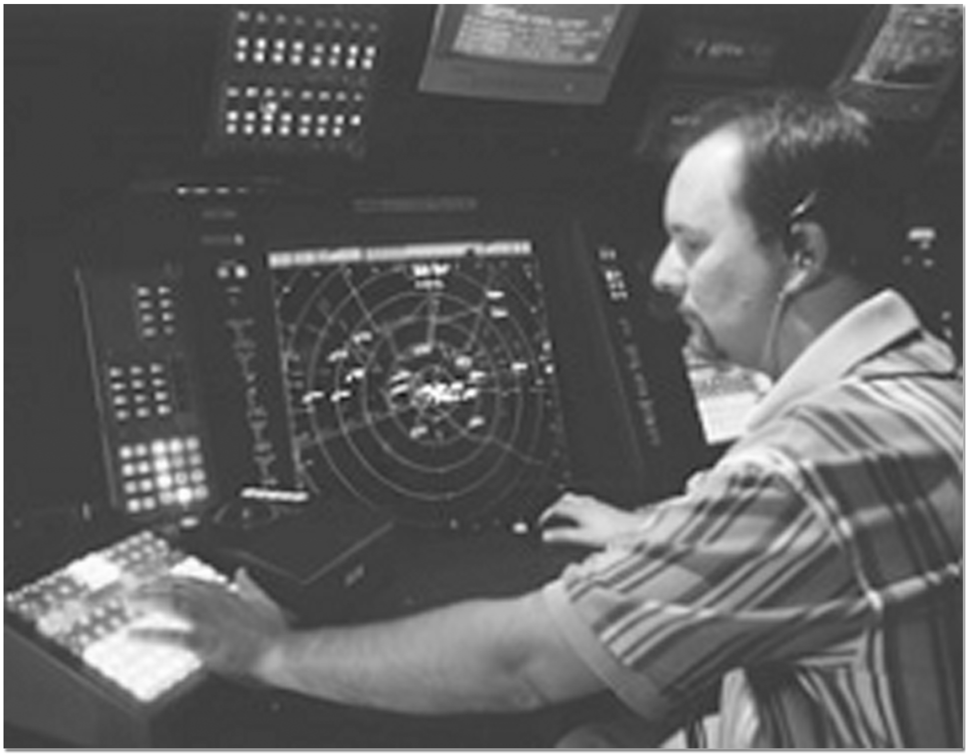


Source: RSPA.

The TIA program is assessing four vulnerabilities:

- *Interdependency of the transportation system with other critical infrastructures:* According to TIA program documentation, the development of alternative fuels, changes in telecommunication technologies, and the evolving financial role of the federal government in the security of privately operated transportation systems are affecting the relationship between the nation's transportation infrastructure and some of the nation's other critical infrastructures. The purpose of this assessment is to describe the current and evolving dependence between the nation's transportation infrastructure and some of the nation's other critical infrastructures including energy, electronic-commerce, banking and finance, and telecommunications. For example, the nation's air traffic control system relies on telecommunications to manage the safety and efficiency of air transportation, as shown in figure 2. Researchers plan to determine the costs, in terms of economic disruption and loss of lives, associated with terrorists exploiting transportation infrastructure vulnerabilities.

Figure 2: An Air Traffic Controller Uses a Digital Radar Display and Workstation Computers Interconnected through Telecommunications Systems for Air Traffic Management



Source: Federal Aviation Administration.

- *Transportation and logistical requirements for emergency response teams in dealing with weapons of mass destruction*: The purpose of this assessment is to evaluate the transportation and logistics assets required in responding to terrorist activities. The assessment will include an analysis of transportation operations and procedures, personnel, supplies, and transportation assets such as vehicles, containers, and pallets. Specifically, researchers plan to analyze the institutional and economic implications of terrorist activities involving weapons of mass destruction in order to develop emergency transportation action plans and compile emergency transportation procedure best practices. Emergency teams were transported to respond to the terrorist attack on the World Trade Center on September 11, 2001, as shown in figure 3.

Figure 3: Emergency Response Teams Transported to the Site of the World Trade Center in New York City Work to Clear Debris After the Terrorist Attack on September 11, 2001

Source: Federal Emergency Management Administration.

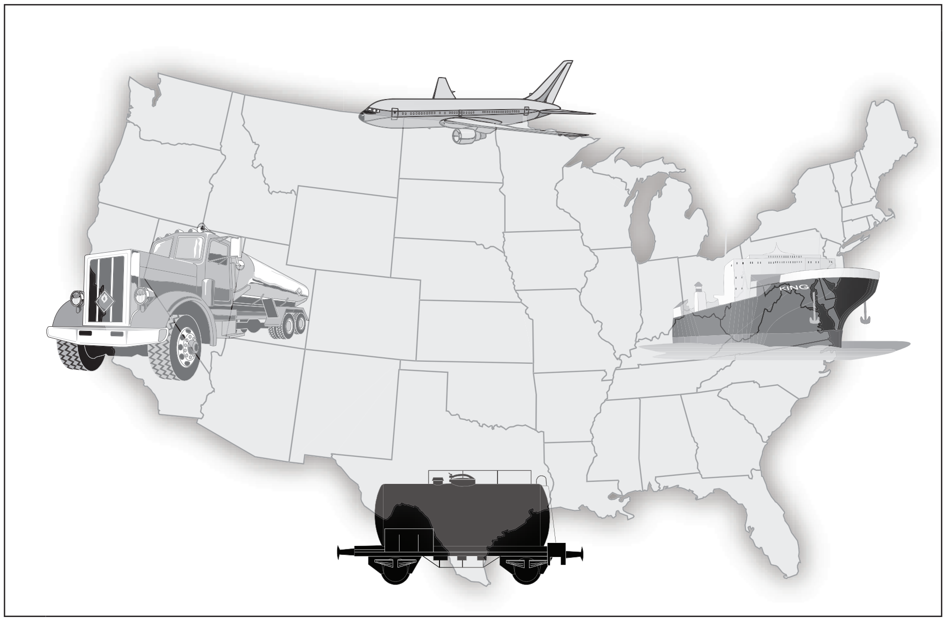
- *Feasibility of alternative backup systems for the global positioning system*: The purpose of this assessment is to provide a continuation of the August 2001 report by the Volpe National Transportation Systems Center, Vulnerability of the Transportation Infrastructure Relying On The Global Positioning System. The report concluded that the global positioning system is vulnerable to both intentional and nonintentional disruption, and identified a need for a backup for the global positioning system. To follow-up on the August 2001 report, researchers plan to analyze and describe the performance, cost, and practicality of backup systems and procedures. Figure 4 shows a picture of a global positioning satellite.

Figure 4: A Global Positioning Satellite

Source: Lockheed Martin Missiles & Space.

- *Options to transition hazardous materials transportation security guidelines to security requirements*: The purpose of this assessment is to evaluate the tradeoffs in the transportation of hazardous materials that exist between security, economic, proprietary, and delivery factors. RSPA plans to provide an analysis and description of these tradeoffs in different threat scenarios for different modes of transportation. Figure 5 provides an overview of the types of transportation being assessed.

Figure 5: Air, Marine, and Surface Modes of Transportation of Hazardous Materials Being Assessed by RSPA



Source: Nova Development Corporation.

RSPA plans to work with OIS to disseminate the results of the program to private transportation system operators and to stakeholders in DOT and other federal agencies through 11 formal reports, presentations, workshops, and the Internet. Table 1 provides an overview of the program's planned products and progress to date.

Table 1: TIA Program Planned Products and Progress to Date

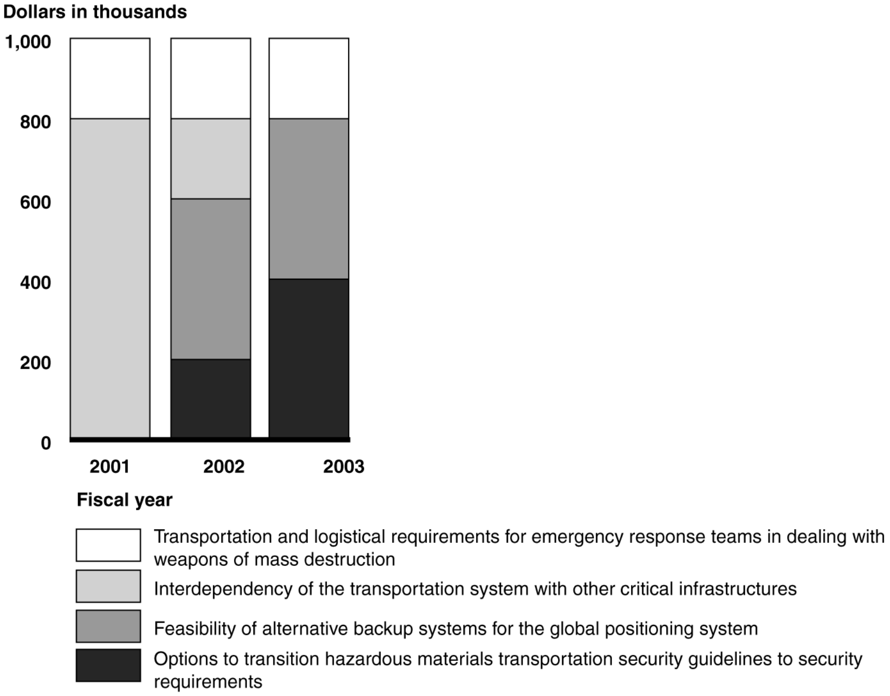
Vulnerability assessments	Planned products and progress to date
Interdependency of the transportation system with other critical infrastructures	**Energy:** • TIA program researchers have drafted a report, "Security Risks Associated with Transportation-Energy Interdependencies," which will be reviewed by OIS. This draft report is intended to illustrate the complexities in defining interdependency vulnerabilities. As of February 2003, this report had not yet been issued. • A second report studying the relationship between electrical distribution infrastructure and transportation is scheduled for completion in May 2003.
	E-Commerce: • TIA program managers are contracting with the Transportation Research Board to develop a report describing information technology in the freight industry, reviewing current freight security practices, and identifying potential vulnerabilities in the freight industry. The report is scheduled for completion in May 2003. • TIA program researchers have completed a background paper, "E-Commerce Vulnerabilities: Impacts on the Transportation System," (March 2002), which presents information on identifying and protecting critical information technology infrastructure, ranking vulnerabilities, and estimating potential impacts (costs) if the vulnerabilities are exploited. TIA researchers have also conducted a briefing on the impact of electronic systems in shaping the future transportation system. An accompanying slide presentation, "Transportation in 2050," has been drafted and is under review.
	Banking & Finance: • TIA program researchers are working on a report, "Economic Effects of the September 11 Terrorist Attacks: A Survey of Current Studies and an Overview of the Implications for Transportation," examining the impact of the events of September 11 on the banking and finance systems and their associated effects on the nation's transportation system. While originally scheduled for release in September 2002, RSPA officials told us that this report is not yet complete and may be discontinued due to its limited value in light of numerous studies conducted on this issue. • A report reviewing the results of other research involving the interdependency of the nation's transportation infrastructure with the nation's banking and finance system is scheduled for completion in spring 2003.
	Telecommunication: • TIA program researchers are finalizing a report on the interdependency between the nation's aviation industry and telecommunications industry. • Additional research is intended to address the interdependence of the nation's telecommunications industry with other nonaviation sectors of the nation's transportation system. According to Volpe Center researchers, this final report is likely to consist of several volumes, each with a specific modal focus. This report is scheduled for completion in May 2003.
Transportation and logistical requirements for emergency response teams in dealing with weapons of mass destruction	• TIA program researchers presented a set of data tables describing the various emergency response teams transportation requirements, including personnel and equipment. According to program researchers, these tables were delivered to RSPA's Office of Emergency Transportation in July 2002. • TIA program researchers have conducted a bio-terrorism conference to aid in identifying gaps in the emergency response system. The conference was held in Washington D.C., on November 19-20, 2002.
Feasibility of alternative backup systems for the global positioning system	• TIA program researchers are working on a report designed to identify and provide cost benefit assessments of alternatives to use in backing up the global positioning system should it be disrupted by sabotage or terrorist attack. The report intends to assist DOT in determining the most appropriate alternative radio-navigation system to use in the nation's transportation system. This report is scheduled for completion in December 2003.

Vulnerability assessments	Planned products and progress to date
Options to transition hazardous materials transportation security guidelines to security requirements	• TIA program researchers reviewed recent literature, workshops, and conferences on security options and implications related to the transportation of hazardous materials. The final report was released in December 2002. • According to program managers, potential areas of work for the second phase of this project include an assessment of the implementation of security plans, and the development of better data on hazardous material shipments with high security concerns. This work is scheduled for completion in December 2003.

Source: RSPA and Volpe Center data.

Congress appropriated $1 million each year to RSPA for the TIA program in fiscal years 2001, 2002, and 2003. Figure 6 provides an overview of the TIA program funding for fiscal years 2001 through 2003 for each of the four vulnerability assessments.

Figure 6: TIA Program Funding by Vulnerability Assessment (Fiscal Years 2001 – 2003)



Source: RSPA and Volpe Center budget data.

RSPA Has Not Fully Coordinated Their Activities with OIS in Selecting the Vulnerabilities to Be Assessed and in Implementing the Assessments for the TIA Program

RSPA has not fully coordinated their activities with OIS—DOT's key transportation security stakeholder—in selecting the vulnerabilities to be assessed or in implementing the assessments for the TIA program. RSPA coordinated with OIS in selecting two vulnerability assessments in fiscal year 2001. Specifically, in fiscal year 2001, RSPA worked with OIS to select one vulnerability for assessment and notified OIS of its selection of a second vulnerability for assessment. RSPA, however, did not coordinate with OIS officials in the selection of two additional vulnerability assessments in fiscal year 2002. RSPA's coordination with OIS during the program's implementation has been limited to only one of the four vulnerability assessments under review.

RSPA's Coordination with OIS in the Selection of the Vulnerabilities to Be Assessed in the TIA Program

RSPA coordinated with OIS and used various criteria, such as PDD 62 and 63, in selecting only two of the four vulnerabilities to be assessed in the TIA program. For example, RSPA consulted with OIS to select one of the two vulnerabilities for assessment in fiscal year 2001 and notified OIS of its selection of a second vulnerability. Specifically, in a memorandum dated March 6, 2001, OIS identified and proposed a list of critical infrastructure protection research requirements for assessment and requested that RSPA address them as a high priority.[3] In this initial proposal, the Director of OIS said that significant OIS involvement would be required to effectively implement the program given its responsibilities for defining transportation security vulnerabilities, ensuring that vulnerability assessments are conducted, and implementing actions to mitigate those vulnerabilities. On April 9, 2001, RSPA issued a memorandum to OIS outlining its research agenda for fiscal year 2001 and stating that OIS's involvement in assuring the program's quality, credibility, and review was critical. This memorandum confirmed RSPA's plans to assess the interdependency of the transportation system with other critical infrastructures, as suggested by OIS's proposed list, and notified OIS of RSPA's intention to conduct a second assessment—the transportation and logistical requirements for emergency response teams in dealing with weapons of mass destruction—that was not included on OIS's list.

[3] In fiscal year 2000, OIS received funding for transportation infrastructure protection activities. In fiscal year 2001, funding in this area of research shifted from OIS to RSPA.

In the aftermath of the terrorist attacks of September 11, 2001, RPSA issued a solicitation on behalf of all DOT modes for additional transportation security technology research and concepts to be included in the TIA program or related transportation security programs. OIS officials participated with RSPA in reviewing the proposals received in response to the solicitation. However, according to the Associate Administrator of RSPA's Office of Innovation, Research, and Education (hereafter referred to as the Associate Administrator), DOT did not receive the funds to pursue any of these proposals.

During fiscal year 2002, RSPA did not coordinate with OIS to determine what additional assessments to select for inclusion in the program. Instead, RSPA selected two transportation vulnerabilities for assessment under the program after holding discussions with Volpe Center researchers and officials from RSPA's Office of Hazardous Materials Safety. While the Associate Director of OIS said he was unaware that additional vulnerabilities had been selected for assessment in fiscal year 2002 prior to our discussions with him regarding the status of the program, he noted that both of these assessments—on the feasibility of alternative backup systems for the global positioning system, and an assessment on options to transition hazardous materials transportation security guidelines to security requirements—were valid and of high priority. According to OIS and RSPA officials, this lack of coordination resulted, in part, from disagreements and misunderstandings about the other's respective role in the program. As indicated by a series of e-mail communications between OIS and RSPA officials during the period between October 2001 and January 2002, questions about the respective roles of OIS and RSPA in the program's management, specific research areas, and the logistics of this research were raised on numerous occasions with no apparent resolution. Neither RSPA nor OIS were able to provide us with documentation to show that these issues were resolved. (See app. II for specific stakeholders involved and criteria used to select the vulnerabilities chosen for assessment under the TIA program in fiscal years 2001 and 2002.)

RSPA's Coordination with OIS in the Implementation of the Assessments in the TIA Program

RSPA's coordination with OIS, DOT's security stakeholder, during the implementation of the TIA program has been limited to one of the four vulnerability assessments. While OIS has participated in meetings regarding the assessment of the options to transition hazardous materials transportation security guidelines to security requirements, RSPA did not similarly involve OIS in the program's three other vulnerability assessments. OIS and RSPA officials said that this lack of coordination during the implementation of the program resulted, in part, from continued disagreements and misunderstandings about the other's respective role in the program. Further, OIS's Associate Director said that because of OIS's lack of involvement in the TIA program, he was not aware of the program's progress to date and therefore expressed uncertainty about whether the program's research is meeting the requirements of PDD 62 and 63.

OIS's Associate Director also said that OIS's working relationships with private industry stakeholders might have helped RSPA obtain industry-sensitive information for the program's assessments. RSPA officials acknowledged that a primary challenge of the TIA program involves obtaining information on industry-specific, competition-sensitive issues. For example, RSPA officials said that private sector owners and operators, such as those from the oil industry, are cautious about releasing proprietary information because of the possibility that this information could be used by (1) business rivals to gain a competitive advantage, (2) terrorists to harm and destroy critical infrastructure, and (3) the federal government to pursue further regulations of the industry. As a result, TIA program researchers told us that they are limited in their ability to identify specific threats and weaknesses relating to some of the specific vulnerabilities under assessment. According to RSPA's Associate Administrator, because of these limitations, the TIA program is, in some instances, examining vulnerability issues on a conceptual level rather than through specific case studies of industry infrastructure. For example, instead of assessing the vulnerabilities of specific privately owned infrastructures, such as oil refineries, RSPA is addressing some critical details of crude oil transport using ports in Louisiana and Texas to illustrate the complexities in defining the interdependency vulnerabilities between the nation's transportation and energy infrastructures. (See app. III for a summary of OIS involvement in the implementation of the TIA program, as well as a listing of all of the significant stakeholders reported by RSPA who were consulted during the implementation of the TIA program.)

We discussed our findings about the lack of coordination with RSPA's Associate Administrator and OIS's Associate Director and suggested they take steps to increase their coordination efforts. They agreed that increased coordination would be beneficial. Specifically, they agreed to hold bi-monthly updates on the progress of each of the vulnerability assessments, discuss program task methodologies and approaches, and identify options for addressing the challenges facing program researchers in conducting the program's vulnerability assessments. The first update was held in March 2003. Furthermore, RSPA's Associate Administrator agreed to provide TSA's Director for Threat Assessment and Risk Management[4] with information on the TIA program's findings, challenges, and lessons learned. In our discussions with TSA's Director for Threat and Risk Assessment, she said that such information regarding the TIA program would be helpful in guiding TSA's future efforts in planning and conducting transportation security research. Because of actions taken by RSPA and OIS to improve coordination we are making no recommendations at this time.

Agency Comments and Our Evaluation

We provided a copy of the draft report to DOT and RSPA officials who agreed with the contents of the report and provided technical clarifications that we incorporated into the report. They did not provide written comments on the report.

We will send copies of this report to the Secretary of Transportation, appropriate congressional committees, and other interested parties. We will also make copies available to others upon request. In addition, the report will be available at no charge on the GAO Web site at http://www.gao.gov.

[4] TSA's Threat Assessment and Risk Management Program was established in October 2002 to provide oversight and assistance regarding threat and vulnerability assessments conducted by TSA. The program also serves to coordinate with other federal agencies to ensure that complete assessments of the vulnerabilities facing the nation's transportation system are conducted.

If you have questions about this report, please call me on (202) 512-2834 or Chris Keisling on (404) 679-1917. Other key contributors included Colin Fallon, Bert Japikse, Steve Morris, and Jason Schwartz.

Katherine Siggerud
Acting Director, Physical Infrastructure Issues

Appendix I: Volpe National Transportation System Center Studies Related to Transportation Infrastructure Assurance

Funding source	Fiscal year	Funding amount	Products
Presidential Commission on Critical Infrastructure Protection	1996	$380,000	**Reports:** • Supervisory Control and Data Acquisition Vulnerabilities (1997) • National Air Space Vulnerabilities (1997) • Traffic (Surface) Central Systems Vulnerabilities (1997) **White Papers:** • Electromagnetic Threats to Rail/Transit Operations (1997)
Department of Defense 1996 Supplemental Appropriation for a Surface Transportation Vulnerability Assessment	1997	$2,400,000	**White Papers:** • Criminal Use of Transportation Infrastructure (1997) • Railroad Bridges and Tunnels Vulnerability (1998) • Railroad Signaling and Control Vulnerability (1998) **Reports:** • Intermodal Cargo Security Best Practices (1999) • Transportation Infrastructure Assurance Research and Development Plan (1999 and 2000)
RSPA Research and Technology and Strategic Planning (Total Terminal Security/TIA Task)	1996	$15,000	**Workshops:** • Emerging Issues in Transportation Information Infrastructure Security (1996) • Global Positioning Study Interference and Mitigation (1998) • Chemical/Biological Incidents (1998) • Marine Safety and Port Security (2000) **Reports:** • Intermodal Cargo Security Best Practices (1999) • Transportation Infrastructure Assurance Research and Development Plan (1999 and 2000)
	1997	$15,000	
	1998	$50,000	
	1999	$35,000	
	2000	$85,000	
	2001	$50,000	
DOT Office of Intelligence and Security	2000	$700,000	**Reports:** • DOT Communications (Security) Reports (2001) • Updated Supervisory Control and Data Acquisition (SCADA) Study (2002) • Global Positioning System Vulnerability Study (2001)

Source: GAO presentation of RSPA and Volpe Center data.

Appendix II: Stakeholders Involved and Criteria Used in Selecting the Vulnerabilities Assessed Under the TIA Program

	Selected in FY 2001		Selected in FY 2002	
Stakeholders involved and criteria used	**Interdependency of the transportation system with other critical infrastructures**	**Transportation and logistical requirements for emergency response teams in dealing with weapons of mass destruction**	**Feasibility of alternative backup systems for the global positioning system**	**Options to transition hazardous materials transportation security guidelines to security requirements**
Stakeholders involved:				
DOT's Office of Intelligence and Security	✓	✓		
RSPA's Office of Emergency Transportation		✓		
RSPA's Office of Hazardous Materials Safety				✓
Volpe National Transportation Systems Center			✓	✓
Criteria used:				
Presidential Decision Directive 62		✓		
Presidential Decision Directive 63	✓			
Critical Foundations, Presidential Commission on Critical Infrastructure Protection (Oct. 1997)	✓			
Critical Infrastructure Research Plan, DOT	✓			
Interim Report on Computer Security, DOT Office of the Inspector General, (July 2000)	✓			
Surface Transportation Vulnerability Assessment, DOT (1999)	✓			
Combating Terrorism: Federal Response Teams Provide Varied Capabilities: Opportunities Remain to Improve Coordination, GAO Report (GAO/NSIAD-01-13)		✓		
Ability to leverage ongoing research and development projects	✓	✓	✓	✓

Source: GAO presentation of RSPA information on TIA program stakeholders involved and selection criteria.

Appendix III: Entities Reported by RSPA Who Were Involved during the Implementation of the TIA Program

		Type of involvement		
Assessment	**Entity involved**	**To obtain information**	**For discussion of task approach**	**For discussion of interim results**
Interdependency of the transportation system with other critical infrastructures	**Office of Intelligence and Security**			
	Federal Aviation Administration			✓
	Louisiana Offshore Oil Port	✓		
	National Research Council Transportation Research Board		✓	
	Transportation Security Administration			✓
Transportation and logistical requirements for emergency response teams in dealing with weapons of mass destruction	**Office of Intelligence and Security**			
	American Association of Railroads	✓		
	American Association of State Highway and Transportation Officials	✓		
	American Public Transportation Association	✓		
	American Red Cross	✓		
	Army Corps of Engineers	✓		
	Association of State and Territorial Health Officials	✓		
	Battelle Memorial Institute	✓	✓	✓
	Centers for Disease Control and Prevention	✓		
	Department of Agriculture	✓		
	Department of Agriculture/Food and Nutrition Service	✓		
	Department of Agriculture/Animal Plant Health Inspection Service	✓	✓	✓
	Department of Defense	✓		
	Department of Energy	✓		
	Department of Health and Human Services	✓		
	Defense Intelligence Agency	✓	✓	✓
	Department of Justice	✓	✓	✓
	Department of State	✓		
	DOT Maritime Academy	✓		
	DOT Office of the General Counsel	✓		
	DOT Regional Emergency Transportation Representative	✓		
	Environmental Protection Agency	✓		
	Federal Aviation Administration	✓		
	Federal Emergency Management Agency	✓		
	Federal Highway Administration	✓		
	Federal Motor Carrier Safety Administration	✓		
	Federal Railroad Administration	✓		

		Type of involvement		
Assessment	Entity involved	To obtain information	For discussion of task approach	For discussion of interim results
	Federal Transit Administration	✓		
	General Services Administration	✓		
	Georgetown University Medical Center	✓	✓	✓
	International Association of Emergency Managers	✓		
	International Association of Fire Chiefs	✓		
	International City/County Management Association	✓		
	Maritime Administration	✓		
	National Association of Counties	✓		
	National Association of State Emergency Medical Service Directors	✓		
	National Defense Transportation Association	✓		
	National Emergency Managers Association	✓		
	National Highway Traffic Safety Administration	✓		
	National Public Transit Association	✓		
	National Research Council Transportation Research Board	✓		
	Office of US Surgeon General	✓		
	RSPA's Office of Emergency Transportation	✓	✓	✓
	Transportation Security Administration	✓		
	University of California, School of Veterinary Medicine	✓	✓	✓
	University of Delaware, Disaster Research Center	✓		
	Urban Search and Rescue Teams	✓		
	US Coast Guard & National Command Center	✓		
	US Forest Service	✓		
	Veterans Administration	✓		
	Volpe National Transportation Systems Center	✓	✓	✓
	Washington DC Department of Health	✓		
	White House Office of Homeland Security	✓		
	White House Special Assistant to the Vice President	✓		

		Type of involvement		
Assessment	**Entity involved**	**To obtain information**	**For discussion of task approach**	**For discussion of interim results**
Feasibility of alternative backup systems for the global positioning system	**Office of Intelligence and Security**			
	Booz-Allen Hamilton	✓		
	DOT Office of the Secretary		✓	✓
	Federal Aviation Administration		✓	✓
	Federal Railroad Administration		✓	✓
	Northrop-Grumman	✓		
	United States Coast Guard		✓	✓
Options to transition hazardous materials transportation security guidelines to security requirements	**Office of Intelligence and Security**		✓	
	American Association of Railroads	✓		
	American Chemistry Council	✓		
	American Institute of Chemical Engineers	✓		
	Bureau of the Census	✓		
	Bureau of Transportation Statistics	✓		
	DOT Office of the Secretary	✓		
	Federal Motor Carrier Safety Administration	✓		
	Federal Railroad Administration	✓		
	General Accounting Office	✓		
	Inland Rivers, Ports and Waterways Association	✓		
	National Transportation Safety Board	✓		
	RSPA's Office of Hazardous Materials Safety		✓	✓
	RSPA's Office of Pipeline Safety	✓		
	Transportation Security Administration	✓		
	US Army Corps of Engineers	✓		
	United States Coast Guard	✓		
	Vanderbilt University	✓		

Source: RSPA.

Note: According to RSPA officials, this list includes significant stakeholders who had input in the TIA program as of March 12, 2003.

(542016)

GAO's Mission

The General Accounting 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 the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to daily E-mail alert for newly released products" under the GAO Reports heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone:	Voice:	(202) 512-6000
	TDD:	(202) 512-2537
	Fax:	(202) 512-6061

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

Public Affairs

Jeff Nelligan, managing director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548