

April 2009

FREIGHT RAIL SECURITY

Actions Have Been
Taken to Enhance
Security, but the
Federal Strategy Can
Be Strengthened and
Security Efforts Better
Monitored



GAO

Accountability * Integrity * Reliability



Highlights of [GAO-09-243](#), a report to congressional requesters

Why GAO Did This Study

An attack on the U.S. freight rail system could be catastrophic because rail cars carrying highly toxic materials often traverse densely populated urban areas. The Department of Homeland Security's (DHS) Transportation Security Administration (TSA) is the federal entity primarily responsible for securing freight rail. GAO was asked to assess the status of efforts to secure this system. This report discusses (1) stakeholder efforts to assess risks to the freight rail system and TSA's development of a risk-based security strategy; (2) actions stakeholders have taken to secure the system since 2001, TSA's efforts to monitor and assess their effectiveness, and any challenges to implementing future actions; and (3) the extent to which stakeholders have coordinated efforts. GAO reviewed documents, including TSA's freight rail strategic plan; conducted site visits to seven U.S. cities with significant rail operations involving hazardous materials; and interviewed federal and industry officials.

What GAO Recommends

Among other things, GAO recommends that TSA reflect all security threats in strategy, strengthen its performance measures, better assess and track actions being taken, and more closely work with some federal stakeholders. DHS generally concurs with our recommendations and has initiated action on some; however, these actions will not fully address all of the recommendations.

To view the full product, including the scope and methodology, click on [GAO-09-243](#). For more information, contact Cathleen Berrick at (202) 512-3404 or berrickc@gao.gov.

FREIGHT RAIL SECURITY

Actions Have Been Taken to Enhance Security, but the Federal Strategy Can Be Strengthened and Security Efforts Better Monitored

What GAO Found

Federal and industry stakeholders have completed a range of actions to assess risks to freight rail since September 2001, and TSA has developed a security strategy; however, TSA's efforts have primarily focused on one threat, and its strategy does not fully address federal guidance or key characteristics of a successful national strategy. Specifically, TSA's efforts to assess vulnerabilities and potential consequences to freight rail have focused almost exclusively on rail shipments of certain highly toxic materials, in part, because of concerns about their security in transit and limited resources. However, other federal and industry assessments have identified additional potential security threats, including risks to critical infrastructure and cybersecurity. Although many stakeholders agreed with TSA's initial strategy, going forward TSA has agreed that including other identified threats in its freight rail security strategy is important, and reported that it is reconsidering its strategy to incorporate other threats. Additionally, in 2004, GAO reported that successful national strategies should identify performance measures with targets, among other elements. TSA's security strategy could be strengthened by including targets for three of its four performance measures and revising its approach for the other measure to ensure greater consistency in how performance results are quantified.

Federal and industry stakeholders have also taken a range of actions to secure freight rail, many of which have focused on securing certain toxic material rail shipments and have been implemented by industry voluntarily; however, TSA lacks a mechanism to monitor security actions and evaluate their effectiveness, and new requirements could pose challenges for future security efforts. GAO's *Standards for Internal Control in the Federal Government* calls for controls to be designed to ensure ongoing monitoring. While the freight rail industry has taken actions to better secure shipments and key infrastructure, TSA has limited ability to assess the impacts of these actions because it lacks a mechanism to systematically track them and evaluate their effectiveness. Having such information could strengthen TSA's efforts to efficiently target its resources to where actions have not been effective. New, mandatory security planning and procedural requirements will also necessitate additional federal and industry efforts and resources, and may pose some implementation challenges for both federal and industry stakeholders.

Federal and industry stakeholders have also taken a number of steps to coordinate their freight rail security efforts; however, federal coordination can be enhanced by more fully leveraging the resources of all relevant federal agencies. GAO previously identified a number of leading practices for effective coordination that could help TSA strengthen coordination with federal and private sector stakeholders.

Contents

Letter		1
	Background	6
	The Federal Government and Industry Have Assessed Threats, Vulnerabilities, and Consequences to Freight Rail, but TSA's Security Strategy Does Not Fully Address Identified Threats or Key Federal Guidance for National Strategies	17
	Federal Efforts Have Guided Voluntary Industry Actions and Generally Focused on TIH, but New Requirements Could Pose Challenges	37
	Stakeholders Have Implemented Several Strategies to Coordinate Their Efforts to Secure the Freight Rail System, but Opportunities Exist to Improve Coordination between Federal Stakeholders and Their Sector Partners	52
	Conclusions	60
	Recommendations for Executive Action	62
	Agency Comments and Our Evaluation	63
Appendix I	Objectives, Scope, and Methodology	68
Appendix II	Federal and Industry Freight Rail Security Vulnerability and Consequence Assessment Activities Conducted since 2001	77
Appendix III	TSA Did Not Consistently Measure Results for Its Key Performance Measure	85
Appendix IV	Summary of Key Actions Taken to Secure Freight Rail	87
Appendix V	Federal and Industry Stakeholders Also Report Facing Technology Challenges to Enhancing the Security of TIH	107

Appendix VI	Summary of 9/11 Commission Act Requirements Pertaining to Freight Rail Security	110
<hr/>		
Appendix VII	Comments from the Department of Homeland Security	115
<hr/>		
Appendix VIII	GAO Contact and Staff Acknowledgments	123

Tables

Table 1: The NIPP Risk Management Framework	14
Table 2: Three Elements of Risk Assessment	16
Table 3: Federal and Rail Industry Assessments Conducted since September 11, 2001, to Determine Freight Rail Security Threats, Vulnerabilities, and Consequences	18
Table 4: Summary of Key Characteristics for a Successful National Strategy and Related Executive Order Factors	29
Table 5: Sector Goals and Freight Rail Subordinate Objectives to Complete Sector Goals	32
Table 6: Key Federal Security Actions Taken since September 11, 2001	39
Table 7: Key Rulemakings and Legislative Requirements Affecting Freight Rail Security	47
Table 8: Key Agreements Signed Involving Federal Agencies and Their Industry Partners	54
Table 9: Formal Committees and Other Entities Established by Federal and Industry Stakeholders to Facilitate Coordination	58
Table 10: Names and Locations of Organizations Contacted	69
Table 11: AAR Industrywide Security Management Plan's Four Alert Levels	100
Table 12: Key Provisions from the 9/11 Commission Act That Are Relevant to Freight Rail Security	110

Figures

Figure 1: Rail Yard in New Jersey Holding Numerous Hazardous Materials Tank Cars	7
Figure 2: Rail Bridge in Louisiana	8
Figure 3: View from Observation Tower at a Rail Yard	43
Figure 4: Camera System Located in the Upper-Right-Hand Corner of the Tunnel	102
Figure 5: Light Towers at a Rail Yard in Houston	102
Figure 6: Perimeter Fencing at a Rail Yard in Houston	103
Figure 7: TIH Rail Customer Facility with Barbed Wire Fencing around the Perimeter	106

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



United States Government Accountability Office
Washington, DC 20548

April 21, 2009

The Honorable Bennie G. Thompson
Chairman
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

The Honorable Corrine Brown
Chair
The Honorable Bill Shuster
Ranking Member
Subcommittee on Railroads, Pipelines, and Hazardous Materials
Committee on Transportation and Infrastructure
House of Representatives

The Honorable Elijah E. Cummings
House of Representatives

Freight railroads are a key component of the nation's transportation network, operating on more than 140,000 miles of track, traversing thousands of bridges and tunnels, and carrying millions of tons of freight annually. As a principal carrier of freight in the United States, freight railroads are vital to the U.S. economy, transporting nearly 13 percent of the nation's goods and generating \$42 billion in annual revenues.¹ Freight railroads carry many major commodities, including coal, grain and other agricultural products, food, steel, motor vehicles, and highly hazardous chemicals, such as chlorine and ammonia. Freight railroad companies are also the primary owners of the infrastructure and rail lines over which they operate and pay billions of dollars each year to construct, maintain,

¹Transportation Security Administration, Transportation Systems Critical Infrastructure and Key Resources Sector-Specific Plan-Freight Rail Modal Annex, May 2007.

and renew their tracks and equipment, according to the Association of American Railroads (AAR).²

While there are currently no specific threats to U.S. freight rail, experts consider the U.S. rail system to be an attractive terrorist target because of its public accessibility, long stretches of open and unattended track, and the difficulty of securing a wide array of rail assets that are difficult to patrol. Further, an attack on the U.S. freight rail system could lead to catastrophic loss of life because the system often traverses densely populated urban areas carrying highly hazardous materials. According to the Department of Transportation (DOT), freight rail is the primary mode by which hazardous materials are transported throughout the nation, with railroads typically carrying from 1.7 million to 1.8 million carloads of hazardous materials annually.³ The category of hazardous materials considered to be the most dangerous to the public are Toxic Inhalation Hazards (TIH), which can be fatal if inhaled. TIH materials include chlorine (used in water treatment) and anhydrous ammonia (used in agriculture).⁴ In addition, shipments of TIH, especially chlorine, frequently move through densely populated areas to reach, for example, water treatment facilities that use these products. If released from a railcar in large quantities under certain atmospheric conditions, TIH materials could result in fatalities to the surrounding population.⁵ For example, an accidental train derailment in Graniteville, South Carolina, in 2005 unintentionally caused the release of several tons of TIH materials into the atmosphere, resulting in nine deaths, the treatment of 75 people for chlorine exposure, and the evacuation of over 5,400 people within a 1-mile

²AAR is a trade association whose membership includes freight railroads that operate 67 percent of the industry's mileage, employ 93 percent of the workers, and account for 95 percent of the freight revenue of all railroads in the United States, and passenger railroads that operate intercity passenger trains and provide commuter rail service.

³Federal hazardous materials transportation law defines a hazardous material as a substance or material that the Secretary of Transportation has determined is capable of posing an unreasonable risk to health, safety, and property when transported in commerce. For emergency response purposes, railcars and containers containing of hazardous materials bear external markings and placards to identify which hazardous materials are being transported. Placards identify the type of hazard the material being shipped poses.

⁴TIH materials are gases or liquids that are known or presumed on the basis of tests to be so toxic to humans that they pose a hazard to health in the event of a release during transportation. See 49 C.F.R. §§ 171.8, 173.115, and 173.132.

⁵For example, chlorine is typically carried in tank cars that can hold up to 90 tons of material, which if released into the atmosphere, may have a lethal dispersal range of over 2 miles.

radius for several days. As a result, concern exists that similar scenarios deliberately executed on a larger scale by terrorist groups could pose serious risks of fatalities and injuries. In addition to the potential for physical harm to the public caused by a hazardous materials release, concern also exists regarding the critical role that certain rail infrastructure plays in the efficient operation of the rail network, including the interdependency of passenger and freight rail networks as a result of shared infrastructure. As such, the degradation or destruction of critical rail infrastructure could potentially have negative economic consequences affecting both passenger and freight rail modes.

Securing the nation's freight rail system is a shared responsibility requiring coordination between multiple stakeholders. Specifically, the Department of Homeland Security's (DHS) National Infrastructure Protection Plan (NIPP) identifies the Transportation Security Administration (TSA) as the sector-specific agency (SSA) responsible for securing all modes of surface transportation, including freight rail.⁶ Furthermore, in 2004, the Homeland Security Council (HSC) requested that DHS and DOT identify and mitigate the security risks associated with the rail transportation of TIH.⁷

You asked us to evaluate the status of federal and industry efforts to secure the freight rail system. In response, this report addresses the following questions: (1) To what extent have federal and industry freight rail stakeholders assessed the risks to the nation's freight rail network, and has TSA developed a risk-based strategy—consistent with applicable federal guidance and characteristics of a successful national strategy for securing the system? (2) What actions have federal and industry

⁶The NIPP, issued by DHS in June 2006 as a requirement of Homeland Security Presidential Directive 7, provides the unifying structure for the integration of critical infrastructure and key resources (CIKR) protection efforts into a single national partnership model. Critical infrastructure includes systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters. Key resources are publicly or privately controlled resources essential to minimal operations of the economy or government, including individual targets whose destruction would not endanger vital systems but could create a local disaster or profoundly damage the nation's morale or confidence. For purposes of this report, we will use the term critical infrastructure to also include key resources. Furthermore, the NIPP also outlines a comprehensive risk management framework that defines critical protection roles and responsibilities for DHS; federal SSAs; and other federal, state, local, tribal, and private sector partners to secure all sectors of the United States.

⁷The HSC was established by the President to ensure the coordination of all homeland security-related activities among executive departments and agencies.

stakeholders taken to secure freight rail systems since September 11, 2001; to what extent has TSA monitored their status and effectiveness; and what, if any, challenges hinder the implementation of future actions?
(3) To what extent have federal and industry stakeholders coordinated their efforts to secure the freight rail system?

To assess the extent to which federal and industry freight rail stakeholders assessed risks to the freight rail system, we reviewed various threat, vulnerability, and consequence assessments prepared by DHS, DOT, and stakeholders outside of the federal government. Although DHS, DOT, and industry characterized these assessments as threat, vulnerability, and consequence assessments, we did not evaluate the quality of the assessments nor did we determine the extent to which the assessments were conducted consistent with requirements outlined in the NIPP as this analysis was outside the scope of our work. However, we did discuss the assessments' reported results with the respective agencies and private entities that conducted them to ascertain the efforts that were made to identify potential threats, vulnerabilities, and consequences associated with an attack on the freight rail system. We analyzed TSA's freight rail security strategy, or strategic plan—the Freight Rail Modal Annex to the Transportation Sector-Specific Plan (TSSP)—to determine the extent to which it addressed the threats, vulnerabilities, and consequences identified in the assessments we reviewed.⁸ To determine the extent to which TSA has developed a risk-based strategy for securing freight rail, we compared TSA's strategy with requirements pertaining to freight rail security assessments in Executive Order 13416, *Strengthening Surface Transportation Security*;⁹ executive guidance, including the NIPP and the TSSP; and GAO's guidance on six desirable characteristics of an effective

⁸The NIPP obligates each sector to develop a sector-specific plan that describes strategies to protect the nation's CIKR under its purview, outline a coordinated approach to strengthen its security efforts, and determine the appropriate programmatic funding levels. The TSSP and its supporting modal implementation plans, or annexes, establish the Transportation Systems Sector's strategic approach based on the tenets outlined in the NIPP and the principles of Executive Order 13416, *Strengthening Surface Transportation Security*. Furthermore, each modal implementation plan, or modal annex, details how each distinct mode intends to achieve the sector's goals and objectives.

⁹Exec. Order No. 13,416, 71 Fed. Reg. 71,033 (Dec. 5, 2006). Executive Order 13416 mandates that an annex shall be completed for each surface transportation mode in support of the TSSP. The Freight Rail Annex was developed to meet this mandate and is intended to meet the minimum content requirements set forth in this order.

national strategy.¹⁰ We also analyzed the methodology and data TSA used to determine how the agency was meeting its main performance goal for freight rail. We had concerns about the reliability of these data, which we discuss later in this report.

To determine federal and industry stakeholder actions taken to secure freight rail, we reviewed documentation, such as summary reports on the results of DHS and DOT freight rail security programs, and requirements in the Implementing Recommendations of the 9/11 Commission Act (9/11 Commission Act).¹¹ We also reviewed relevant TSA and DOT rail safety and security rulemakings at various stages of development.¹² We conducted site visits in seven major U.S. cities where TSA has conducted freight rail security assessments or where railroads handle significant TIH rail shipments and interviewed federal and industry stakeholders about actions taken and the challenges they faced in implementing such actions. As part of our site visits, we also monitored all three phases of TSA's Corridor Review in Chicago, Illinois, to better understand the process and specific security actions taken through these reviews.¹³ During our site visits we also met with officials from the seven largest freight railroads.¹⁴ Because we selected a nonprobability sample of cities and railroads, the results from these visits cannot be generalized to all U.S. cities or used to make inferences about the views of all freight railroad officials. However, the results from these visits provided us with a broad perspective of the types of actions taken to secure freight rail and the challenges operators face in doing so. During our site visits, we also discussed specific actions

¹⁰GAO, Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism, [GAO-04-408T](#) (Washington, D.C.: Feb. 3, 2004).

¹¹Pub. L. No. 110-53, 121 Stat. 266 (2007).

¹²73 Fed. Reg. 72,182 (Nov. 26, 2008); 73 Fed. Reg. 72,130 (Nov. 26, 2008); 73 Fed. Reg. 20,752 (Apr. 16, 2008); 73 Fed. Reg. 17,818 (Apr. 1, 2008); 71 Fed. Reg. 76,852 (Dec. 21, 2006); and 71 Fed. Reg. 76,834 (Dec. 21, 2006).

¹³TSA's Corridor Reviews are vulnerability assessments that focus on the security risks posed by TIH rail shipments in major cities. We discuss these assessments in detail later in our report.

¹⁴These railroads are known as Class I railroads. A Class I railroad is defined by the U.S. Surface Transportation Board as a railroad company that earns adjusted annual revenue of \$319.3 million or more. Class I freight railroads represent about 93 percent of railroad freight revenue and 69 percent of the total U.S. rail mileage. Currently, seven railroads in North America are classified as Class I railroads. They are CSX, BNSF, Canadian National, Canadian Pacific, Norfolk Southern, Union Pacific Railroad, and Kansas City Southern Railway.

individual railroads had taken to secure their shipments and infrastructure and any challenges they faced in implementing these as well as potential future actions. We also reviewed available agency documentation regarding the type and scope of federal and industry actions taken to secure freight rail, and we reviewed our Standards for Internal Control in the Federal Government to further assist us in evaluating TSA's efforts to monitor and evaluate the effectiveness of actions taken.¹⁵ To determine the extent to which freight rail stakeholders have been coordinating security efforts, we analyzed several memorandums of understanding (MOU) and cooperation that affect freight rail security as well as specific mechanisms stakeholders have implemented to coordinate their security efforts, and compared these actions with criteria for coordination included in the NIPP as well as leading practices for collaborating agencies.¹⁶ We also met with federal and industry officials to discuss their views on coordination among freight rail security stakeholders.

We conducted this performance audit from February 2007 through April 2009 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Appendix I contains more details about our scope and methodology.

Background

The Freight Rail System Is Inherently Vulnerable

Certain characteristics of the freight rail system make it inherently vulnerable and therefore difficult to secure. Specifically, America's rail network is an open system, with expanses of infrastructure spread over vast regions, and often traverses densely populated urban areas. In addition, railroads operate in large and small rail yards and along narrow rights-of-way containing thousands of miles of track that are generally unprotected by fences or other barriers. As a result, freight trains and

¹⁵GAO, *Standards for Internal Control in the Federal Government*, [GAO/AIMD-00-21.3.1](#) (Washington, D.C.: November 1999).

¹⁶GAO, *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, [GAO-06-15](#) (Washington, D.C.: Oct. 21, 2005).

individual railcars can be especially difficult to secure in transit as shipments move from their points of origin to their destinations. Trains and railcars often travel across multiple railroads and rail lines and sometimes sit for periods of time on rail tracks or in rail yards awaiting further shipment. At points of connection, freight cars will typically sit in rail yards until they can be moved into a train with the same destination as the freight. This can be of particular concern for railcars carrying hazardous materials, since many rail yards and storage locations are located close to densely populated areas and may contain dozens of loaded hazardous materials tank cars at any given time. Also, the difficulty and cost associated with physically securing rail yards can leave these cars accessible to trespassers. Figure 1 shows a rail yard holding numerous hazardous materials tank cars.

Figure 1: Rail Yard in New Jersey Holding Numerous Hazardous Materials Tank Cars



Source: GAO.

Furthermore, the interdependency of freight and passenger rail infrastructure—including common bridges, tunnels, control centers, tracks, signals, and switches—increases the likelihood that incidents affecting highly critical assets could affect the entire system, including both freight and passenger rail carriers. Numerous passenger and commuter rail systems throughout the country operate at least partially over tracks or rights-of-way owned by freight railroads. For example, Amtrak—the sole provider of intercity passenger rail transportation in the United States—operates on more than 22,000 miles of track owned by

freight railroads through operating agreements.¹⁷ As a result, certain assets are particularly critical to the operation of the rail system. For example, control centers are a key factor to the railroads' ability to manage their networks. Thus, an attack on a control center could have widespread consequences. Moreover, certain bridges, such as those over large rivers, play a key role in the national railroad system because capacity constraints limit options to reroute trains. As a result, incidents limiting or preventing their use could negatively affect the economy by severely delaying rail traffic for significant periods of time and causing transportation system delays and disruption. Figure 2 shows a key rail bridge in Louisiana, which is only one of a few rail bridges that go over the Mississippi River.

Figure 2: Rail Bridge in Louisiana



Source: DHS.

Multiple Stakeholders Share Responsibility for Securing Freight Rail Systems

Securing the nation's freight rail system is a shared responsibility requiring coordination between multiple federal and industry stakeholders.

¹⁷In addition, many commuter and light rail systems operate primarily or exclusively over tracks owned by freight railroads.

Federal Government Stakeholders

Within the federal government, DHS and DOT share responsibility for securing the freight rail system. Prior to the terrorist attacks of September 11, 2001, DOT was the primary federal entity involved in regulating freight rail transportation. In response to the September 11, 2001, attacks, Congress passed the Aviation and Transportation Security Act of 2001 (ATSA), which created and conferred upon TSA broad responsibility for securing all modes of transportation, including the freight rail system.¹⁸ Within TSA, the Transportation Sector Network Management (TSNM) office manages all surface transportation security issues, with divisions dedicated to each surface mode of transportation, including freight rail.¹⁹ In addition, TSA's Office of Intelligence (OI) is responsible for collecting and analyzing threat information for threats affecting the entire transportation network. In 2002, Congress passed the Homeland Security Act, which established DHS, transferred TSA from DOT to DHS, and assigned DHS responsibility for protecting the nation from terrorism, including securing the nation's transportation systems.²⁰ Finally, in 2007, the 9/11 Commission Act was signed into law, which requires DHS to establish several programs aimed at improving freight rail security.²¹ The law requires that DHS, among other things, identify high-risk railroads and issue regulations requiring high-risk railroads to conduct vulnerability assessments and develop security plans, establish a program for conducting security exercises for railroad carriers, and issue regulations for a security training program for frontline rail employees.

Within DHS, the National Protection and Programs Directorate (NPPD), through the DHS Office of Infrastructure Protection (IP), is responsible for coordinating efforts to protect the nation's most critical assets across all 18 sectors, including the transportation sector.²² Within the transportation

¹⁸Pub. L. No. 107-71, § 101(a), 115 Stat. 597, 597 (2001).

¹⁹The TSNM office was established in November 2005 following internal restructuring of the modal offices. Prior to 2005, freight rail security was addressed through the Freight Rail Division of the Intermodal Program Office.

²⁰Pub. L. No. 107-296, 116 Stat. 2135 (2002).

²¹Implementing Recommendation of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, 121 Stat. 266 (2007).

²²The 18 industry sectors are 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, postal and shipping, public health and healthcare, transportation, and water.

sector, DHS IP works with TSA to identify nationally critical freight rail assets. The Federal Emergency Management Agency (FEMA) is responsible for allocating and managing DHS grants for freight rail, primarily through the DHS IP Buffer Zone Protection Program (BZPP) and TSA's freight rail security grant program.²³ While federal stakeholders play a role in facilitating risk-based infrastructure security efforts, implementation of asset-specific protective security measures remains the responsibility of individual asset owners/operators, mostly individual railroads.

DHS funding for freight rail security consists of a general appropriation to TSA for its entire surface transportation security program, which includes commercial vehicle and highway infrastructure, rail and mass transit, pipeline, and freight rail security and appropriations to FEMA for its State Homeland Security Grant Program and Infrastructure Protection Program.²⁴ Annual appropriations to TSA for its surface transportation security program were \$36 million in fiscal year 2006, \$37.2 million in fiscal year 2007, \$46.6 million in fiscal year 2008, and \$49.6 million in fiscal year 2009. FEMA funding available under the two principal grant programs ranged from about \$2 billion to \$2.5 billion for each fiscal year from 2006 through 2009.

Although TSA has primary responsibility for freight rail security, DOT maintains a regulatory role with respect to the transportation of hazardous

²³The Post-Katrina Emergency Management Reform Act of 2006 was enacted as Title VI of the Department of Homeland Security Appropriations Act, 2007, and transferred many functions of the former Preparedness Directorate, including managing certain grant programs, to FEMA. Pub. L. No. 109-295, 120 Stat. 1355, 1394, 2006. We discuss BZPP and the freight rail security grant program later in the report.

²⁴The State Homeland Security Grant Program consists of three underlying programs that have been used, in part, to finance freight rail security enhancements—the State Homeland Security Program, the Urban Area Security Initiative, and the Law Enforcement Terrorism Prevention Program. The State Homeland Security Program provides funds to build capabilities at the state and local levels through planning, equipment, training, and exercise activities. The Urban Area Security Initiative focuses on the unique planning, equipment, training, and exercise needs of high-threat, high-density urban areas. The Law Enforcement Terrorism Prevention Program provides resources to law enforcement and public safety communities to support critical terrorism prevention activities, including establishing and enhancing fusion centers and collaborating with non-law enforcement partners, other government agencies, and the private sector. Under the Infrastructure Protection Program, freight rail security efforts have been funded through BZPP. BZPP is a targeted grant program that provides funding to states to purchase equipment that will enhance security measures around critical infrastructure facilities for all modes of transportation, which we discuss later in the report.

materials via rail.²⁵ Specifically, the Homeland Security Act clarified DOT's responsibility to include ensuring the security, as well as the safety, of the transportation of hazardous materials.²⁶ Within DOT, the Pipeline and Hazardous Materials Safety Administration (PHMSA) is responsible for developing, implementing, and revising security plan requirements for hazardous materials carriers, while inspectors from the Federal Railroad Administration (FRA) enforce these regulations in the rail industry through periodic reviews of the content and implementation of these security plans.²⁷

In 2003, PHMSA issued regulations intended to strengthen the security of the transportation of hazardous materials.²⁸ The regulations require persons who transport or offer for transportation certain hazardous materials to develop and implement security plans.²⁹ Security plans must assess the security risks associated with transporting these hazardous materials and include measures to address those risks.³⁰ The regulations also require that all employees who directly affect hazardous materials

²⁵49 U.S.C. § 5103.

²⁶Pub. L. No. 107-296, § 1711, 116 Stat. 2135, 2319-20 (2002) (codified at 49 U.S.C. § 5103).

²⁷FRA conducts freight rail-related inspections. FRA acts under the delegation of the Secretary of Transportation. 49 C.F.R. § 1.49(s).

²⁸49 C.F.R. § 172.700-172.804.

²⁹Specifically, the subset of hazardous materials requiring security plans includes (1) a highway route-controlled quantity of a Class 7 (radioactive) material; (2) more than 25 kilograms (55 pounds) of Division 1.1 (explosive with a mass explosion hazard), 1.2 (explosive with a projection hazard), or 1.3 (explosive with predominately a fire hazard) material; (3) more than 1 liters (1.06 quarts) per package of a TIH material of a specified concentration level; (4) a shipment of hazardous materials in bulk packaging having a capacity of 13,248 liters (3,500 gallons) or more for liquids or gases or more than 13.24 cubic meters (468 cubic feet) for solids; (5) a shipment in other than bulk packaging of 2,268 kilograms (5,000 pounds) gross weight or more of one class of hazardous materials for which placarding is required; (6) a select agent or toxin regulated by the Centers for Disease Control and Prevention; and (7) a quantity of hazardous materials that requires placarding. 49 C.F.R. § 172.800 (2007). PHMSA proposed a rule in September 2008 that would narrow the list of hazardous materials subject to the security plan regulations. 73 Fed. Reg. 52,558 (Sept. 9, 2008).

³⁰At a minimum, a plan must include measures to (1) confirm information provided by job applicants hired for positions that involve access to and handling of hazardous materials covered by the security plan, (2) respond to the assessed risk that unauthorized persons may gain access to hazardous materials covered by the security plan, and (3) address the assessed risk associated with the shipment of hazardous materials covered by the security plan from origin to destination.

transportation safety receive training that provides awareness of security risks associated with hazardous materials transportation and of methods designed to enhance transportation security. Such training is also to instruct employees on how to recognize and respond to possible security threats. Additionally, each employee of a firm required to have a security plan must be trained concerning the plan and its implementation. As described below, PHMSA issued a new regulation on November 26, 2008, to further enhance the security and safety of the rail movement of certain hazardous materials, including shipments of certain explosive, TIH, and radioactive materials.³¹

Industry Stakeholders

A number of national organizations and coordination groups exist to represent the broad composition of freight rail security stakeholders, which include seven national (Class I) railroads and hundreds of other railroad companies that operate over shorter distances, known as regional (Class II) or short line (Class III) railroads.³² In addition to the railroads, chemical companies, such as BASF and Dow Chemical, ship highly hazardous materials via U.S. rail networks and also play a role in ensuring the safety and security of their rail shipments. Some industry organizations also play a role in disseminating pertinent information, such as threat communications from DHS and DOT, to their members. For example, AAR has played a key role in representing the interests of member railroads by establishing a Rail Alert Network to coordinate security actions industrywide. AAR also routinely collaborates with federal entities to assist its members in enhancing freight rail security.

In the freight rail industry, under many circumstances, rail carriers may be required to transport hazardous materials and bear many of the costs associated with ensuring the safety and security of these rail shipments. Under what is known as common carrier obligations, freight rail carriers

³¹73 Fed. Reg. 72,182 (Nov. 26, 2008). Specifically, carriers subject to the new regulations include those that ship (1) more than 2,268 kilograms (5,000 lbs.) in a single carload of a Division 1.1, 1.2, or 1.3 explosive; (2) a quantity of a material poisonous by inhalation in a single bulk packaging; and (3) a highway route-controlled quantity of a Class 7 (radioactive) material. 49 C.F.R. § 172.820(a).

³²Class II and III railroads include a number of short line railroads that provide freight rail transportation. A short line is an independent railroad company that operates over a relatively short distance. Class II railroads earn annual revenue from \$25.5 million to \$319.3 million, and Class III railroads are those earning less than \$25.5 million. Regional and short line railroads generally exist for one of three reasons: to link two industries requiring rail freight together; to interchange revenue traffic with other, usually larger, railroads; or to operate a tourist passenger train service.

must provide transportation or service upon reasonable request.³³ While shipments of materials such as TIH account for about 1 percent of all railroad business, railroad representatives reported that insurance premiums associated with the transportation of TIH materials account for over 50 percent of their insurance costs. Chemical companies we met with also reported an increase in shipping rates associated with transporting TIH as well as other costs associated with implementing security measures to protect hazardous material rail shipments as required by the DHS Chemical Facility Anti-Terrorism Standards Program.³⁴

A Risk-Based Approach to Freight Rail Security

In recent years, we, along with Congress (most recently through the Intelligence Reform and Terrorism Prevention Act of 2004), the executive branch (e.g., in presidential directives), and the 9/11 Commission have required or advocated that federal agencies with homeland security responsibilities utilize a risk management approach to help ensure that finite national resources are dedicated to assets or activities considered to have the highest security priority. We have concluded that without a risk management approach, there is limited assurance that programs designed to combat terrorism can be properly prioritized and focused. Thus, risk management, as applied in the homeland security context, can help to more effectively and efficiently prepare defenses against acts of terrorism and other threats.

Homeland Security Presidential Directive 7 (HSPD-7) directed the Secretary of Homeland Security to establish uniform policies, approaches, guidelines, and methodologies for integrating federal infrastructure protection and risk management activities. Recognizing that each sector possesses its own unique characteristics and risk landscape, HSPD-7 designates a federal government SSA for each of the critical infrastructure sectors that are to work with DHS to improve critical infrastructure

³³Pursuant to law regarding common carrier obligations, rail carriers must provide transportation or service upon reasonable request. 49 U.S.C. § 11101. This obligation stems from, among other things, the concept that an entity that represents to the public that it provides transportation of certain goods and that such transportation is available to the general public has a duty to shippers and to the general public to receive and transport such goods.

³⁴The DHS Chemical Facility Anti-Terrorism Standards Program requires certain chemical facilities that are determined to be high risk to complete site security plans that include measures that satisfy DHS's risk-based performance standards.

security.³⁵ On June 30, 2006, DHS released the NIPP, which created a risk-based framework for the development of SSA strategic plans, in accordance with HSPD-7.³⁶ As the SSA for transportation, TSA developed the TSSP 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 (NSTS).³⁷ The TSSP contains supporting modal implementation plans for each transportation mode, including the freight rail mode, which provides information on current efforts to secure freight rail as well as TSA's overall goals and objectives related to freight rail security.

The NIPP defines roles and responsibilities for security partners in carrying out critical infrastructure and key resources protection activities through the application of risk management principles. Table 1 provides details on the interrelated activities of the risk management framework as defined by the NIPP.

Table 1: The NIPP Risk Management Framework

Set security goals	Define specific outcomes, conditions, end points, or performance targets that collectively constitute an effective protective posture.
Identify assets, systems, networks, and functions	Develop an inventory of the assets, systems, and networks that comprises the nation's critical infrastructure, key resources, and critical functions. Collect information pertinent to risk management that takes into account the fundamental characteristics of each sector.

³⁵DHS serves as the SSA for 11 sectors: information technology; communications; transportation systems; chemical; emergency services; nuclear reactors, material, and waste; postal and shipping; dams; government facilities; commercial facilities; and critical manufacturing. Other SSAs are the Departments of Agriculture, Defense, Energy, Health and Human Services, the Interior, and the Treasury and the Environmental Protection Agency. See GAO, *Critical Infrastructure Protection: Sector Plans and Sector Councils Continue to Evolve*, [GAO-07-706R](#) (Washington, D.C.: July 10, 2007).

³⁶HSPD-7 requires DHS and DOT to collaborate on all matters related to transportation security and transportation infrastructure protection.

³⁷The NSTS, mandated in the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), outlines the federal government approach—in partnership with state, local, and tribal governments and private industry—to securing the U.S. transportation system from terrorist threats and attacks.

Set security goals	Define specific outcomes, conditions, end points, or performance targets that collectively constitute an effective protective posture.
Assess risks	Determine risk by combining potential direct and indirect consequences of a terrorist attack or other hazards (including seasonal changes in consequences and dependencies and interdependencies associated with each identified asset, system, or network), known vulnerabilities to various potential attack vectors, and general or specific threat information.
Prioritize	Aggregate and analyze risk assessment results to develop a comprehensive picture of asset, system, and network risk; establish priorities based on risk; and determine protection and business continuity initiatives that provide the greatest mitigation of risk.
Implement protective programs	Select sector-appropriate protective actions or programs to reduce or manage the risk identified, and secure the resources needed to address priorities.
Measure effectiveness	Use metrics and other evaluation procedures at the national and sector levels to measure progress and assess the effectiveness of national CIKR.

Sources: GAO and DHS.

The NIPP requires that federal agencies use information collected through the risk management framework to inform the selection of risk-based priorities and continuous improvement of security strategies and programs to protect people and critical infrastructure through the reduction of risks from acts of terrorism. Within the risk management framework, the NIPP also establishes baseline criteria for conducting risk assessments. According to the NIPP, risk assessments are a qualitative determination of the likelihood of an adverse event occurring, a quantitative determination of the likelihood of such an event, or both, and are a critical element of the NIPP risk management framework. Risk assessments help decision makers identify and evaluate potential risks so that countermeasures can be designed and implemented to prevent or mitigate the effects of the risks. The NIPP characterizes risk assessment as a function of three elements: threat, vulnerability, and consequence. Information from these elements can lead to a risk characterization and provide input for prioritizing security goals. Table 2 provides specific information on these three elements.

Table 2: Three Elements of Risk Assessment

Threat	The likelihood that a particular asset, system, or network will suffer an attack or an incident. In the context of risk from terrorist attack, the estimate of this is based on the analysis of the intent and the capability of an adversary; in the context of natural disaster or accident, the likelihood is based on the probability of occurrence.
Vulnerability	The likelihood that a characteristic of, or flaw in, an asset's, system's, or network's design, location, security posture, process, or operation renders it susceptible to destruction, incapacitation, or exploitation by terrorists or to other intentional acts, mechanical failures, and natural hazards.
Consequence	The negative effects on public health and safety, the economy, public confidence in institutions, and the functioning of government, both direct and indirect, that can be expected if an asset, system, or network is damaged, destroyed, or disrupted by a terrorist attack, natural disaster, or other incident.

Source: GAO.

The Federal Government and Industry Have Assessed Threats, Vulnerabilities, and Consequences to Freight Rail, but TSA's Security Strategy Does Not Fully Address Identified Threats or Key Federal Guidance for National Strategies

Federal and industry stakeholders have completed a range of threat, vulnerability, and consequence assessments for freight rail since September 11, 2001, and TSA has developed a strategy for securing freight rail.³⁸ However TSA's efforts have largely focused exclusively on TIH rail shipments despite the identification of other potential threats to freight rail infrastructure and cybersecurity systems. TSA officials stated that the agency focused on securing TIH for several reasons, including limited resources and the HSC's decision in 2004 to prioritize TIH as a key risk requiring federal attention. While other federal and industry freight rail stakeholders have agreed that focusing on TIH was a sound initial strategy because it is a key potential rail security threat and an overall transportation safety concern, there are other security threats for TSA to consider and evaluate as its freight rail strategy matures, such as potential sabotage to critical infrastructure. In addition, TSA's security strategy does not fully address characteristics that we have previously identified as key practices for successful national strategies, such as having targeted performance measures to gauge results or related factors outlined in Executive Order 13416, such as the identification of lead, support, and partner roles. Specifically, three of the four performance measures in TSA's Freight Rail Modal Annex to the TSSP do not identify any specific targets to gauge the effectiveness of federal and industry programs in achieving the measures or the transportation sector security goals outlined in the annex. Moreover, TSA has been limited in its ability to measure the impact federal and industry efforts are having in achieving the agency's key performance measure for the freight rail program because the agency was unable to obtain critical data necessary to consistently measure results.

³⁸ Although federal and industry stakeholders categorized these efforts as threat, vulnerability, and consequence assessments, we did not evaluate them to determine whether they met the NIPP criteria for threat, vulnerability, and consequence assessments. As a result, we discuss them in this report using the terminology that federal and industry stakeholders used to identify them.

Since 2001, Federal and Industry Stakeholders Have Conducted a Range of Threat, Vulnerability, and Consequence Assessments, but TSA's Security Efforts Have Largely Focused on TIH Rail Shipments

Since September 11, 2001, federal and industry stakeholders have conducted a range of threat, vulnerability, and consequence assessments for freight rail; however, of the federal assessment efforts completed to date, TSA's have focused almost exclusively on TIH, while others focused on more than just one threat. For example, federal threat assessments considered multiple capabilities and tactics an adversary may employ to attack the freight rail system, while the vulnerability and consequence assessments were mixed—TSA's focused exclusively on TIH as the threat, while other federal and industry assessments included other areas of risk, such as the vulnerabilities and consequences associated with critical infrastructure or cyberattacks.³⁹ See table 3 for a summary of the various federal and industry assessments conducted since 2001. For more information on these assessments, see appendix II.

Table 3: Federal and Rail Industry Assessments Conducted since September 11, 2001, to Determine Freight Rail Security Threats, Vulnerabilities, and Consequences

Entity	Time frame	Description	Risk components		
			T	V	C
Threat assessments					
TSA OI	2003-present	Freight rail threat assessments: Analysis of threat information from relevant foreign and domestic sources; include discussions of plausible threat scenarios. These assessments are developed annually and provide an overview of threats, including possible attack tactics and targets to the freight rail system and its infrastructure (e.g., bridges and tunnels).	X		
Vulnerability and consequence assessments focusing on TIH					
PHMSA	2003	TIH Summary Report: Vulnerability and consequence assessment of 13 specific TIH materials. PHMSA chose these materials because of, among other things, the volume carried on the railroads and the toxicity of the 13 chemicals. The purpose of the assessment was to better define the potential harm that could result from an attack on a TIH railcar, and determine some of the general weaknesses of TIH railcars and how a terrorist may breach one.		X	X

³⁹A threat scenario is a potential terrorist event that delineates the tactics and locations a terrorist may use, for example, to cause casualties or disrupt the economy, using expert judgment based on available risk information, including past attacks.

Entity	Time frame	Description	Risk components		
			T	V	C
TSA Freight Rail TSNM office	2004-present	Rail Corridor Reviews: Assessments that determine the vulnerabilities and potential consequences posed by TIH cars in major urban areas by identifying locations within a city's rail network where TIH cars are vulnerable to a terrorist attack. TSA also developed a systematic methodology to quantitatively rate security risks at locations.		X	X
TSA Freight Rail TSNM office	2007-present	TIH Rail Risk Reduction Program: Rail TIH transportation security assessment in 46 major urban areas that uses industry data about TIH car movements inside the urban area. TSA also audits the security status of the cars while at rail yards, and assesses potential consequences to the surrounding population.		X	X
Other vulnerability and consequence assessments					
Freight rail industry	2001-2008	Freight rail security assessment: Analysis of the railroad industry's vulnerabilities and consequences in five major areas: hazardous materials, critical infrastructure, information systems, military shipments, and rail operations.		X	X
TSA Freight Rail TSNM office	2007-present	Corporate Security Reviews (CSR): Analysis of rail carrier security plans and corporate-level procedures to enhance domain awareness and identify vulnerabilities of Class I railroads, initially, and, subsequently, short line railroads.		X	
DHS IP	2006-present	<p>Prioritized critical infrastructure list: Identification of nation's CIKR across all sectors, including freight rail assets such as bridges, tunnels, and cyber-dispatch centers. Assets that appear on this list are chosen based on criteria established by DHS IP in concert with TSA.</p> <p>Infrastructure vulnerability assessments: Assessments intended to provide DHS and other stakeholders with detailed vulnerabilities of infrastructure for all CIKR sectors (including freight rail infrastructure) to develop and prioritize mitigation efforts. Assessments are one of two categories:</p> <p>Site Assistance Visit (SAV): Facility-level assessment conducted by DHS IP in partnership with asset owners.</p> <p>BZPP: Assessment conducted around the buffer area of the asset. BZPP reviews are conducted by local law enforcement in coordination with DHS IP. The assessments focus on identifying locations and weaknesses from which terrorists may conduct surveillance or launch an attack on an asset.</p>			X

Source: GAO analysis of DHS, DOT, and industry data.

Legend: T = threat; V = vulnerability; C = consequence.

TSA's Threat Assessments Have Identified Multiple Threats to Freight Rail

Note: TSA, DHS IP, and PHMSA characterize completed assessments as threat, vulnerability, and consequence assessments; we did not evaluate the quality of these assessments or the extent to which they were conducted consistent with requirements outlined in the NIPP. DHS also determined that the criteria and specific numbers related to the prioritized critical infrastructure list are "For Official Use Only." As a result, these data are not contained in this report.

TSA's threat assessments have identified multiple potential threats to freight rail, such as attacks on TIH rail shipments or destruction of and sabotage to key infrastructure; however, TSA has previously reported that there was no specific information that extremist groups or individuals are planning to conduct an act of terrorism against the U.S. freight rail system. TSA's OI has conducted periodic threat assessments since 2003 and completed its most recent assessment in May 2008. These assessments have mostly been scenario based, meaning they focus on potential attack scenarios that might be successful in destroying or exploiting freight rail assets or systems.⁴⁰ According to TSA officials, this is the best available technique for conducting these threat assessments, given the lack of specific threat information related to freight rail. TSA officials also reported that the threat scenarios identified in the 2008 freight rail threat assessment primarily resulted from discussions and concerns about the potential consequences and vulnerabilities associated with the identified scenarios. Possible threats included hazardous materials attacks, such as the breaching of a TIH tank car; destruction of or sabotage to freight rail bridges and tunnels; and cyberattacks to the rail system that could disrupt or cause the degradation of railroads' signaling and dispatching systems.

The NIPP guidance states that risk assessments should provide a means to estimate the likelihood of a threat occurring. However, TSA officials said that calculating these values for freight rail is difficult because of the lack of specific threat information. Despite the difficulties of doing so, it is important for TSA to use available information to attempt to estimate the likelihood of a threat occurring to the freight rail system because estimating the likelihood of various threats occurring, as directed by the NIPP, could provide TSA with additional information with which to assess

⁴⁰In addition to modal-specific threat assessments, TSA OI develops other threat-related products for groups inside and outside of TSA. For instance, the office leads daily Administrator's briefings to discuss current and ongoing threats to the transportation sector, including freight rail. Also, TSA OI collects and disseminates suspicious incidence reports to make stakeholders aware of recent suspicious activity that may be terrorism related.

TSA and PHMSA Have Conducted Several Vulnerability and Consequence Assessments Focusing Exclusively on TIH Rail Shipments

overall risks to freight rail assets and systems.⁴¹ Although TSA has not estimated the likelihood of various threats occurring, the agency has prioritized certain threat scenarios as well as the overall threat to freight rail compared to other modes. TSA officials have concluded, based on their expert judgment and interpretation of available vulnerability and potential consequence information, that the threat of an attack to a TIH car in a high-threat urban area is the highest risk to freight rail.⁴² In addition, the HSC identified the rail transportation of TIH materials as a key security risk. According to a former Deputy Homeland Security Advisor to the President, this position was based on the inherent openness and vulnerability of the rail system, combined with the HSC's review of modeling studies that estimated the potential for significant public harm associated with a large TIH release in a highly populated area. TSA officials also told us that based upon available information, the overall threat of an attack to freight rail is relatively lower than the threat to other modes of transportation, including passenger rail, mass transit, and aviation modes. TSA reported that it based this conclusion primarily on the lack of specific threat information related to freight rail, expert judgment, and the lack of precedent for terrorist attacks using freight rail as compared to other modes.

Since 2003, both TSA and PHMSA have assessed the vulnerabilities and potential consequences associated with an attack on TIH rail shipments. According to TSA, it focused these assessments on TIH because the HSC identified TIH as a security risk that the government needed to address during 2002 and 2003. As directed by the HSC, in 2003, PHMSA conducted an assessment of the vulnerabilities and potential consequences

⁴¹In calculations for risk analysis, the term threat is an estimated value that approximates the likelihood that a specific asset, system, network, sector, or region will suffer an attack or an incident. This differs from "threat scenarios" or "threat analysis," which are generalized descriptions of potential methods of attack that are used to help inform consequence and vulnerability assessments. The NIPP also states that assessments should provide numerical values for estimated consequences, vulnerabilities, and threats whenever possible.

⁴²TSA uses the term high-threat urban area to describe geographic areas that warrant special consideration with respect to transportation security. TSA derived its list of high-threat urban areas from the Urban Areas Security Initiative (UASI) program. Under the UASI program, DHS designates metropolitan areas as high-threat urban areas based on a consideration of the relative threat, vulnerability, and consequences from acts of terrorism faced by each metropolitan area. Specifically, DHS identified UASI areas as high-threat urban areas if they had populations greater than 100,000 and had reported threat data during the past fiscal year.

associated with transporting certain TIH materials by rail.⁴³ For more information on this assessment, see appendix II.

Shortly thereafter, in 2004, the HSC requested that TSA begin more specific assessments, called Corridor Reviews, which focused exclusively on identifying the vulnerabilities and potential consequences posed by TIH rail shipments in 9 major U.S. cities.⁴⁴ As of March 2009, TSA had completed Corridor Reviews in 12 cities, including all 9 cities originally selected for review in 2004, and has reported that the agency will continue conducting these reviews in 48 additional cities that have TIH rail shipments. For a complete discussion of the Corridor Reviews, see appendix II.

More recently, in 2007, TSA began further assessing the potential risk posed by TIH rail shipments in high-threat urban areas by gathering and quantifying vulnerability and consequence information through a project called the TIH Rail Risk Reduction Program. TSA officials stated that the agency developed this assessment program to measure the impact federal and industry efforts are having on achieving the agency's key performance measure for the freight rail security program, which is to reduce the risk associated with the transportation of TIH in major cities, identified as high-threat urban areas, by 50 percent by the end of 2008. According to TSA, this information also gives the agency a way to closely compare the vulnerabilities and consequences related to TIH transportation across various cities over time.⁴⁵ For more information on this assessment, see appendix II.

⁴³ While TSA has determined the specific results of this assessment to be "For Official Use Only," the assessment generally concluded that transporting TIH materials by rail poses a risk in highly populated areas.

⁴⁴TSA officials told us that the initial 9 cities were chosen because they were large population centers with both large rail networks and significant quantities of TIH traveling through them by rail. TSA used aggregate data on city population and the quantities of TIH being transported in each city for the year 2000 to assist in selecting the cities. The 9 cities originally selected in 2004 for TSA Corridor Reviews were Buffalo, Chicago, Cleveland, Houston, Los Angeles, New Orleans, Newark, Philadelphia, and Washington, D.C. TSA officials said that they intend to conduct Corridor Reviews in all major cities that have TIH rail shipments and qualify for DHS's UASI grant program. Several agencies have participated in these security assessments, including DHS IP and DOT's FRA and PHMSA.

⁴⁵As of November 2008, TSA has reported measuring an overall reduction in risk of over 60 percent across all high-threat urban areas. However, we discuss concerns about the accuracy of this measurement later in this report.

Federal and Industry Stakeholders Have Also Conducted Vulnerability and Consequence Assessments Associated with Other Threats

As discussed in table 3, federal and industry stakeholders have also conducted vulnerability and consequence assessments associated with other threats—such as attacks on rail critical infrastructure and cyberattacks. These assessments ranged from narrow assessments of one geographic area, specific asset, or rail carrier to broader assessments that reviewed and ranked critical assets and infrastructure nationwide. For more information on these assessments, see appendix II.

Federal Assessment Efforts

DHS IP has conducted vulnerability and consequence assessments of freight rail assets that focused on security threats other than TIH. For example, DHS IP has developed a prioritized list of critical U.S. infrastructure, including freight rail assets, that if destroyed or disrupted, cause national or regional catastrophic effects.⁴⁶ While TSA and DHS IP work together to develop criteria for determining which assets belong on the list, TSA has not taken steps to assess the security preparedness of these assets. However, after we raised this issue in late 2008, TSA reported in February 2009 that it intends to do so. Further, DHS IP has also conducted more detailed assessments of some of these assets through the BZPP program. However, TSA has not used the results of these assessments to inform its security strategy. Using the results of these assessments could help TSA, as the SSA for freight rail, further inform and refine its freight rail security strategy to ensure the security preparedness of high-priority freight rail assets. TSA officials told us that they understand the importance of securing critical freight rail infrastructure from terrorist attack and are reconsidering the agency's approach for addressing threats to infrastructure in light of completed federal and industry assessments.

In 2007, TSA conducted CSRs of all seven Class I railroads' security plans to determine their compliance with TSA guidelines.⁴⁷ Unlike TSA's TIH-focused Corridor Reviews, a CSR is a broad review that assesses a railroad

⁴⁶Although this list informs the allocation of the BZPP grants, and the determination to conduct SAVs, informing those programs is not the primary reason DHS conducts the process. The department develops the list to fulfill legislative and NIPP requirements to do so, as well as to ensure the nation's leadership have standing lists of the country's most critical infrastructure for risk and incident management purposes.

⁴⁷These reviews assessed the security plans and procedures against the following TSA guidelines: threat assessment and processing; vulnerability assessments; personnel security, auditing/testing of plan; drills/exercises; infrastructure security; hazardous materials security; cybersecurity; and infrastructure security. TSA believes that at minimum, these elements must be in a security plan for industry to effectively respond to a security incident or event.

carrier's security plan and the level of implementation of security countermeasures in several key areas. While these reviews provide TSA with an opportunity to review railroad critical infrastructure information included in a company's security plan, they do not provide information on the security preparedness of specific freight rail infrastructure assets deemed nationally critical, particularly those that have been identified through DHS IP's efforts. TSA officials stated that they plan to eventually use the CSR results to compile a list of industry best practices and to develop security plan baseline standards for a future security plan regulation.

Industry Assessment Efforts

In addition to federal assessment efforts, the freight rail industry has also taken steps to independently assess security risks to the rail network and its operations. The rail industry conducted the first freight rail risk assessment shortly after September 11, 2001, which identified security risks to the entire rail network. Although the assessment, led by AAR, identified specific hazardous materials that were the most dangerous, including TIH materials, it also identified other vulnerabilities and consequences—including those associated with the destruction or degradation of freight rail infrastructure, such as key bridges, tunnels, tracks, and operation centers that electronically direct and monitor train movements. In 2008, the rail industry updated its security assessment to account for changes in the railroads' operating environment since 2001, including the development of an updated list of critical infrastructure as well as cybersecurity vulnerabilities and concerns. The updated assessment resulted in the industry identifying and prioritizing over 1,000 of its rail assets, such as bridges, tunnels, and control centers.⁴⁸ For more information on the rail industry risk assessment and assessments conducted by individual railroad companies, see appendix II.

⁴⁸To prioritize railroad assets, the rail industry developed a formula to score the asset value, which is determined by quantifying the security vulnerabilities and consequences for each asset. Assets considered at most risk generally were those that were (1) difficult to repair or replace, (2) likely to affect a railroad's ability to operate, and (3) lacking effective countermeasures to reduce the likelihood of causing this damage.

TSA's Freight Rail Security Strategy Focuses on One Threat and Does Not Fully Address Key Characteristics of a Successful National Strategy and Factors Outlined in Executive Order 13416

TSA's Freight Rail Strategy Focuses Almost Exclusively on TIH and Does Not Address Other Identified Threats

Since its inception, TSA's Freight Rail Program Office has focused its freight rail security strategy almost exclusively on the threats posed by TIH rail shipments, and the agency does not yet have a strategy for addressing other identified threats. TSA officials said that they intentionally focused on TIH transportation for a number of reasons. For example, TSA officials reported that in 2003, when TSA's freight rail office was first established, the HSC had recommended that DOT, TSA, and other federal agencies focus on securing TIH because the HSC had asserted that transporting TIH by rail was a significant public security risk. Additionally, TSA officials and other federal officials reported that studies had been conducted during that time identifying the transportation of TIH as a significant security risk to public health. For instance, a 2003 study conducted by the Naval Research Lab determined that up to 100,000 people could be injured or killed in Washington, D.C., if the contents of a chlorine tank car were released under worst-case conditions.⁴⁹ While most officials that we interviewed questioned the severity of the study's casualty estimates, they agreed that a large TIH release in an urban setting could cause mass casualties.

TSA program officials also reported on several other issues that also influenced how they set their early priorities for securing freight rail, such as heightened media coverage regarding the ease with which individuals could access TIH railcars and the possible public health impacts of a TIH release. Specifically, news sources in 2002 and 2003 noted security concerns and vulnerabilities related to transporting TIH by railcars in urban areas. Environmental groups had also raised concerns regarding the

⁴⁹Most officials that we interviewed questioned how realistic the results of this study would be in the event of a chlorine tank car breach because it used a worst-case scenario model.

possible dangers of shipping TIH chemicals by rail. Adding to TSA's concerns, which included managing its responsibility and authority for securing freight rail, around 2005 several cities proposed legislation to reroute or limit the transportation of TIH in their jurisdictions. Specifically, cities such as Cleveland, Baltimore, Chicago, and Washington, D.C., had proposed legislation that would prohibit rail companies from carrying TIH through their jurisdictions. Given its legal authorities and responsibilities, TSA officials believed that the agency needed to act to preempt local jurisdictions from creating their own potentially conflicting regulations. Rail industry officials we spoke with said that they had supported this approach, having recognized that they would have to manage multiple requirements across the various jurisdictions that their trains carrying TIH traversed if local jurisdictions created their own regulations. According to TSA officials, the agency's ability to develop a broader strategy was also affected by the lack of personnel in its Freight Rail Program Office, which had only four permanent staff members assigned to it in 2003.⁵⁰ Given this staffing level, TSA officials said that they initially lacked the resources to develop a broader strategy that would include other risks, and that securing TIH shipments was a sound initial focus. Security officials we interviewed from six of the seven Class I railroads agreed that TIH security was a sound initial focus for TSA's freight rail security strategy, because TIH was a key security concern and remains a concern today.⁵¹

TSA describes its strategic focus on TIH in the Freight Rail Modal Annex, identifying the transportation of these commodities as having the greatest potential consequence to harm the public and the economy. However, while the annex has identified both the primary threat scenario and two systematic security gaps—namely, security awareness training and a lack of a robust, standardized corporate security planning for railroads—TSA has not addressed other risks that have been identified through threat, vulnerability, and consequence assessments. In particular, the annex does not contain an approach for mitigating threats to infrastructure, including major freight rail bridges, tunnels, and other assets, nor does it discuss

⁵⁰According to TSA, the office has since expanded to 15 staff members in 2008. TSA's permanent staff assigned to freight rail security was 7 in 2004, 10 in 2005, 12 in 2006, and 15 in 2007. Prior to 2003, TSA organized its freight rail security division differently, but had 3 personnel assigned to freight rail security-related work.

⁵¹One Class I railroad representative that we interviewed told us that securing critical freight rail infrastructure should have been TSA's initial focus.

cybersecurity risks, even though these risks have been identified collectively through TSA threat assessments, DHS IP vulnerability and consequence assessments, and the rail industry's nationwide rail risk assessment. For instance, freight rail stakeholders told us that if certain key bridges were destroyed, the flow of commerce could be severely affected, causing delays and shortages in the delivery of raw materials and other goods used for day-to-day living. Also, rail industry stakeholders said that replacing certain key bridges could take months and cost millions of dollars. Moreover, freight rail stakeholders told us that protecting computer networks and other information systems helps ensure that trains do not collide or switch lines improperly, which could cause derailments of hazardous materials and destruction of major infrastructure. Stakeholders also said that without restricting access to electronic information, such as waybills and other specific commodity information, terrorists could obtain this information to determine the location of TIH tank cars to target them and thereby maximize the impact of an attack on the surrounding population.⁵²

The NIPP states that each SSA should consider threats, vulnerabilities, and consequences in developing its programs and activities. Moreover, since the Freight Rail Modal Annex's publication, the federal government enacted the 9/11 Commission Act, which specifies that the transportation modal security plan required under 49 U.S.C. § 114(s) (in this case, the Freight Rail Modal Annex) must include information on threats, vulnerabilities, and consequences for its respective mode.⁵³ TSA has acknowledged that reflecting all identified threats to freight rail in the agency's strategy is important, and reported that the agency is in the process of reconsidering its security strategy to incorporate other threats as it updates its plan to meet the requirements of the NIPP.⁵⁴ TSA officials stated that they intend to incorporate information from other security assessments that identify additional threats unrelated to TIH transportation, such as TSA OI's identification of cybersecurity as a potential target for a terrorist attack and DHS IP's prioritized critical infrastructure list. While TSA officials recognize that the focus of their

⁵²A waybill is a shipping document that travels with a shipment; identifies the shipper, receiver, origin, and destination; describes the goods; and shows their weight and freight.

⁵³Pub. L. No. 110-53, § 1202(a), 121 Stat. 266, 381 (2007).

⁵⁴The NIPP requires sector-specific plans (which include the TSSP and the Freight Rail Modal Annex) to be reissued every 3 years concurrently with the NIPP, which was to be updated by March 2009.

TSA's Freight Rail Modal Annex Does Not Fully Address Key Characteristics of a Successful National Strategy and Related Factors Outlined in Executive Order 13416

actions has been limited to securing TIH shipments, they also told us that they understood their responsibility under ATSA for securing all aspects of the freight rail sector and were aware of the new requirements in the 9/11 Commission Act, which require the agency to take broader actions. As TSA matures and moves forward with its rail security efforts, a strategy that includes all threat, vulnerability, and consequence information will help the agency make more informed decisions and provide more comprehensive strategies. Furthermore, the 9/11 Commission Act, signed into law in 2007, requires DHS to establish several programs aimed at strengthening freight rail security. These requirements will likely further influence TSA to expand its strategy and will also require the agency to have a greater regulatory oversight role.⁵⁵

While TSA's Freight Rail Modal Annex contains some information that is consistent with our prior work on characteristics of a successful national strategy and that is called for by Executive Order 13416, it lacks other information that if incorporated, could strengthen the annex. Our prior work identified six key characteristics of successful national strategies, many of which are consistent with factors included in Executive Order 13416, which is directed specifically at strengthening surface transportation security.⁵⁶ These characteristics can assist responsible parties, such as TSA, in further developing and implementing the nation's freight rail strategy, as well as enhancing its usefulness in resource and policy decisions to better ensure accountability. Where applicable, we also discuss relevant sections of Executive Order 13416 to highlight the importance of fulfilling these measures to strengthen the freight rail security national strategy. Table 4 briefly describes five of the national strategy characteristics and relevant Executive Order elements that are discussed further below.⁵⁷

⁵⁵For example, the law requires that DHS, among other things, identify high-risk railroads and issue regulations requiring high-risk railroads to develop vulnerability assessments and security plans; establish a program for conducting security exercises for railroad carriers; and issue regulations for a security training program for frontline rail employees.

⁵⁶[GAO-04-408T](#).

⁵⁷The sixth characteristic is problem definition and risk assessment, which addresses the particular national problems and threats the strategy is directed toward mitigating. However, because we provided details earlier in our report on the steps federal and industry stakeholders have taken to assess risks to the freight rail system, we do not address this characteristic in this section of our report.

Table 4: Summary of Key Characteristics for a Successful National Strategy and Related Executive Order Factors

Purpose, scope, and methodology: Addresses why the strategy was produced, the scope of its coverage, and the process by which it was developed. A strategy might discuss the specific impetus that led to its creation, such as statutory requirements, executive mandates, or other events—like terrorist attacks. In addition to describing what it is meant to do and the major functions, mission areas, or activities it covers, a national strategy would ideally also outline its methodology, such as discussing the principles or theories that guided its development, what organizations or offices drafted the document, whether it was the result of a working group, or which parties were consulted in its development.

Organizational roles, responsibilities, and coordination: Addresses which organizations will implement the strategy, their roles and responsibilities, and mechanisms for collaboration. This information considers who is in charge, not only during times of crisis but also during all phases of combating terrorism, including prevention, vulnerability reduction, and response and recovery. This entails identifying the specific federal entities involved and, where appropriate, the different levels of government or stakeholders, such as state and local governments and private entities. Executive Order 13416 also calls for the Secretary of Homeland Security to develop modal annexes that include a description of the respective roles, responsibilities, and authorities of federal, state, local, and tribal governments. A strategy could also describe the organizations that will provide the overall framework for accountability and oversight, identify specific processes for collaboration, and address how any conflicts would be resolved.

Goals, subordinate objectives, activities, and performance measures: Addresses what the strategy is trying to achieve, steps to achieve those results, as well as the priorities, milestones, and performance measures to gauge results. At the highest level, a strategy could provide a description of an ideal “end state,” followed by a logical hierarchy of major goals, subordinate objectives, specific activities, and performance measures to achieve results.^a Executive Order 13416 directs TSA to evaluate the effectiveness and efficiency of current surface transportation security initiatives and calls for the annex to identify processes for assessing compliance with security guidelines and requirements and for assessing the need for revision of such guidelines and requirements to ensure their continuing effectiveness—something that could be accomplished with defined performance measures.

Resources, investments, and risk management: Addresses what the strategy will cost, the sources and types of resources and investments needed, and where resources and investments should be targeted based on balancing risk reductions with costs. Ideally, a strategy would identify criteria and appropriate mechanisms to allocate resources, such as grants, in-kind services, and loans, based on identified needs. Executive Order 13416 directs TSA to use security grants authorized by law to assist in implementing security requirements and guidelines issued pursuant to law. Pursuant to this characteristic, such grants may be included in the modal annex. Alternatively, the strategy might identify appropriate “tools of government,” such as regulations, tax incentives, and standards, or stimulate nonfederal organizations to use their unique resources.

Integration and implementation: Addresses how a national strategy relates to other strategies’ goals, objectives, and activities and to subordinate levels of government and their plans to implement the strategy. For example, a national strategy could discuss how its scope complements, expands upon, or overlaps with other national strategies. Also, related strategies could highlight their common or shared goals, subordinate objectives, and activities. Executive Order 13416 requires that the modal annex identify existing security guidelines and requirements. A strategy could address its relationship to other agency strategies using relevant documents from implementing organizations, such as strategic plans, annual performance plans, or annual performance reports that the Government Performance and Results Act of 1993 (GPRA) requires of federal agencies. A strategy might also discuss, as appropriate, various strategies and plans produced by the state, local, or private sectors and could provide guidance, for example, on the development of national standards, to more effectively link the roles, responsibilities, and capabilities of the implementing parties.

Source: GAO.

^aA goal (also known as a strategic goal or objective) constitutes a specific set of policy, programmatic, and management objectives for the programs and operations covered in the strategic plan, and serves as a framework from which the annual objectives and activities are derived. A goal is expressed in a manner that allows a future assessment to be made regarding whether the goal was or is being achieved. Subordinate objectives assist in focusing the mode’s programs and activities to meet the goals. Activities are specific programs and actions to achieve the subordinate objectives. Performance measures are particular values or characteristics used to measure output or outcome of activities, objectives, and goals.

Purpose, Scope, and Methodology

Although TSA's Freight Rail Modal Annex identifies the purpose and scope of the annex and references several principal documents used to develop the annex—including the Freight Rail Government Coordinating Council (FRGCC) charter, the TSSP, and the NIPP—it does not describe the process or methodology that was used to develop the annex or who developed the annex. For example, the annex states that TSA's vision is to protect the nation's freight rail network from terrorist or criminal attacks and prevent terrorists or other criminals from using freight rail conveyances and their cargoes as weapons of mass effect to attack the public or critical infrastructure. The annex also discusses the scope and type of various federal and industry freight rail security efforts and aligns them with three broad DHS security goals for the transportation sector, as outlined in the TSSP.⁵⁸ In addition, the TSSP also discusses the NIPP as the unifying structure for securing all of the various sectors, including transportation, and discusses several domestic and international terrorist attacks that have occurred as evidence of the various security risks to the transportation sector.⁵⁹ However, the annex does not explain the methodology used in its development, as called for in our prior work on characteristics of a national strategy. For example, while the annex references the NIPP and TSSP as providing the principles or theories that guided its development, the annex does not describe the process and information that were used to develop the strategy or identify which organizations or entities contributed to its development, which could make the document more useful to the organizations responsible for implementing it, as well as to oversight organizations such as Congress.

Organizational Roles, Responsibilities, and Coordination

The Freight Rail Modal Annex addresses this characteristic to only a limited degree. For example, while the annex identifies some stakeholder responsibilities, it does not identify lead, support, and partner roles as called for in Executive Order 13416. Specifically, the Freight Rail Modal Annex identifies some stakeholders' responsibilities, such as identifying

⁵⁸These sector goals are (1) prevent and deter acts of terrorism using or against the transportation system, (2) enhance the resiliency of the U.S. transportation system, and (3) improve the cost-effective use of resources for transportation security.

⁵⁹These incidents include, but are not limited to, the September 11, 2001, attacks on the World Trade Center and the Pentagon; attacks on transportation targets in the 2005 London bombings; and coordinated attacks on four commuter trains in Madrid in 2004.

FRGCC as the primary mechanism for establishing policies, guidelines, and standards, and that the council is to coordinate with industry through the Freight Rail Sector Coordinating Council (FRSCC). The annex also states that TSA, FRA, and PHMSA have signed MOUs to maintain good intragovernmental relationships, and identifies what entities were responsible for conducting past actions to secure freight rail. However, the annex does not identify the roles of federal and nonfederal stakeholders, such as the TSA Freight Rail Security Division, DHS IP, FRA, PHMSA, and the rail industry, in meeting identified freight rail security goals. The inclusion of these subjects in a freight rail security strategy could be useful to agencies and other stakeholders in fostering coordination and clarifying specific roles, particularly where responsibilities overlap or where there are security gaps. Defining specific roles and responsibilities is especially important given the multiple federal and industry stakeholders involved in securing freight rail and the scope and complexity of the rail network.

Goals, Subordinate Objectives, Activities, and Performance Measures

In conformance with this characteristic, the Freight Rail Modal Annex identifies individual transportation sector-wide goals that apply to all modes of transportation, and it also identifies subordinate objectives to clarify how these goals will be met for the freight rail mode, as illustrated in table 5. For each subordinate objective, TSA presents information to explain what the agency, other federal components, or industry is doing to meet the subordinate objective. For instance, the agency identifies its Corridor Reviews and CSRs as activities to accomplish implementing flexible, layered, and effective security programs using risk management.

Table 5: Sector Goals and Freight Rail Subordinate Objectives to Complete Sector Goals

Goals and objectives	Description
Sector goal	Prevent and deter acts of terrorism using or against the transportation system.
Subordinate objectives	<ul style="list-style-type: none"> • Implement flexible, layered, and effective security programs using risk management. • Increase vigilance of freight rail workers. • Enhance information and intelligence sharing among freight rail security partners.
Sector goal	Enhance resiliency of the U.S. transportation system.
Subordinate objectives	<ul style="list-style-type: none"> • Manage and reduce risk associated with key nodes, links, and flows within critical transportation systems to improve overall network survivability. • Enhance the capacity for rapid and flexible response and recovery to all-hazards events.
Sector goal	Improve the cost-effective use of resources for transportation security.
Subordinate objectives	<ul style="list-style-type: none"> • Align sector resources with the highest-priority security risks using both risk and economic analyses as decision criteria. • Ensure robust sector participation in the development and implementation of public sector programs for freight rail protection. • Ensure coordination and enhanced risk-based prioritization of research, development, testing, and evaluation efforts.

Source: GAO analysis of TSA information.

While TSA has also developed performance measures for its freight rail program, their usefulness in helping the agency determine the extent to which its sector goals are being met is limited by the lack of key data to appropriately measure results and key elements typically associated with effective performance measures. Ensuring that all necessary data are included will help ensure that TSA is reporting consistent results, which could help the agency more effectively prioritize its and industry’s resources for securing freight rail. In its Freight Rail Modal Annex, TSA includes an outcome measure—to cumulatively reduce the risk of TIH transportation in major cities by 50 percent by the end of 2008—that contains both a target, or goal, and a specific time frame for achieving the

goal.⁶⁰ The agency also established additional yearly targets for this measure to cumulatively reduce the risk of TIH by a total of 81 percent by the end of 2013.⁶¹ TSA considers this measure its key overall performance indicator for the freight rail security program, and has reported its progress in meeting this indicator to Congress on several occasions. However, we have concerns about this performance measure's reported results because TSA was unable to obtain critical data necessary to consistently calculate cumulative results for this measure over the time period for which it had calculated them—from 2005 to 2008. In particular, some baseline data needed to cumulatively calculate results for this measure are historical and could not be collected. As a result, the agency used a method for estimating risk for its baseline year that was different than what it used for calculating results for subsequent years.

Although TSA made efforts to reconstruct the missing data as well as it could by conducting interviews with relevant rail officials and using its and industry's expert judgment to develop an estimated baseline, any results reported using this measure depend on the collective accuracy, judgment, and recollection of industry officials, rather than on the timely collection of the relevant data. Moreover, our analysis of the data that TSA collected for subsequent years (to calculate the changed condition in risk between the baseline and subsequent years) did not resolve our questions regarding the accuracy of the estimated baseline data. Specifically, in 2007, the first year TSA measured risk for this performance measure, the agency applied the same data estimate of 80 percent to 23 of the 45 cities assessed in place of the baseline 2005 risk information it could not obtain.⁶² However, when TSA surface inspectors had conducted site visits to these

⁶⁰ Outcome measures describe the intended result of carrying out a program or activity. They define an event or condition that is external to the program or activity and that is of direct importance to the intended beneficiaries, the public, or both. An output measure describes the level of activity to be provided over a period of time, including a description of the characteristics (e.g., timeliness) established as standards for the activity.

⁶¹ TSA established annual goals in its submission to the Office of Management and Budget Performance and Rating Tool for TSA's program to strengthen surface transportation security. TSA's goals by year are 55 percent by 2009, 61 percent by 2010, 67 percent by 2011, 74 percent by 2012, and 81 percent by 2013.

⁶² While TSA identified 46 high-threat urban areas in its Rail Security Notice of Proposed Rulemaking and Final Rail Security Rule, the agency only reported on 45 cities related to meeting its goal of reducing TIH risks in 2007. Additionally, 5 cities do not have TIH materials traveling through them by rail. As a result, TSA does not measure TIH risks in those cities. In addition, TSA's 80 percent estimate represents the estimated amount of time TIH railcars were unattended by rail employees during the baseline time period.

same cities to gather this information, the data the inspectors gathered varied greatly by city raising questions regarding the validity of TSA's estimate and the appropriateness of applying the same estimate of risk uniformly to 23 cities. Furthermore, the agency was unable to account for any specific rail carrier actions that would explain why the data varied greatly by city and from the agency's original estimate. As a result, any cumulative results reported using this measure are of questionable accuracy because the agency did not calculate results consistently. This is particularly important because TSA has reported results from this measure to Congress—indicating that over a 60 percent risk reduction had been achieved for freight rail from 2005 through 2008.

GPRA requires agencies to establish goals and targets to define the level of performance to be achieved by a program and express such goals in an objective, quantifiable, and measurable form.⁶³ In addition, we have previously reported that to the greatest extent possible, performance measures should be reasonably free of significant bias or manipulation that would distort the accurate assessment of performance and should not allow subjective considerations or judgments to dominate the outcome of the measurement, which could distort the measure.⁶⁴ Furthermore, performance measures should provide a reliable way to assess progress such that the same results would be achieved if applied repeatedly to the same situation. Likewise, errors in the accuracy of the data could skew the results and affect conclusions regarding the extent to which performance goals have been achieved. Therefore, the usefulness of agency performance information depends to a large degree on the reliability of performance data. While TSA had limited ability to collect some of the relevant data for its baseline year, the agency has been able to collect the relevant data in a timely manner since 2007. As a result, TSA would have the necessary data to consistently measure results on an annual basis and a cumulative basis—provided that the baseline year for any of these calculations is 2007 or later. This approach would allow TSA to produce

⁶³Pub. L. No. 103-62, 107. Stat 285 (1993). GPRA was intended to address several broad purposes, including strengthening the confidence of the American people in their government; improving federal program effectiveness, accountability, and service delivery; and enhancing congressional decision making by providing more objective information on program performance.

⁶⁴GAO, *Tax Administration: IRS Needs to Further Refine Its Tax Filing Season Performance Measures*, [GAO-03-143](#) (Washington, D.C.: Nov. 22, 2002). In this report, GAO reported on nine key attributes of successful performance measures. Among these attributes are objectivity and reliability of measures.

reliable results for the key performance measure for its freight rail security program. Furthermore, while TSA made significant efforts to reconstruct and estimate the data it could not obtain, without more certainty about the data's accuracy and the resulting risk measures, TSA may not know the degree to which its and industry's security efforts have been effective. As a result, it may be less able to ensure the effective and efficient use of resources. Appendix III provides additional information on the data TSA was unable to obtain for this measure.

In addition to concerns about measurable data for this performance measure, TSA lacks specific milestones or targets for its other three measures included in the Freight Rail Modal Annex and time frames for completing more long-term activities, such as TSA's reviews of freight railroad security plans and procedures. For example, one of the three performance measures listed in the annex is an output measure, the "number of completed Corridor Reviews in DHS-designated high-threat urban areas."⁶⁵ However, TSA does not provide any targets or time frames for this measure to identify the number of Corridor Reviews the agency expects to complete or time frames to gauge progress toward completion.

In addition, the subordinate objectives in the annex do not have performance measures associated with them to show progress in meeting the sector goals. For instance, as shown in table 5, TSA developed three subordinate objectives to show progress in meeting the third sector goal of improving the cost-effective use of resources for transportation security. However, the annex contains no performance measures or targets to link the effectiveness of these subordinate objectives in achieving the sector goal. We have previously reported that the linkage between long-term goals and subordinate objectives is important because without this linkage, agency managers and Congress may not be able to judge whether an agency is making annual progress toward achieving its long-term goals.⁶⁶ GPRA also supports this point, stating that performance indicators are the reference markers used to measure whether a goal is being achieved and to measure output or outcome.

⁶⁵TSA's remaining performance measures are (1) percentage of carrier-adopted security action items and (2) percentage of employees who have received security awareness training.

⁶⁶GAO, *Agencies' Annual Performance Plans Under the Results Act: An Assessment Guide to Facilitate Congressional Decisionmaking*, GAO/GGD/AIMD-10.1.18 (Washington, D.C.: February 1998).

Resources and Investments

While the Freight Rail Modal Annex has one section devoted to grant programs and identifies how the grants align with requirements in Executive Order 13416, it does not include freight rail security resources that originate in other programs, such as DHS IP's BZPP, which grants money to local authorities to protect critical infrastructure, nor does it identify priorities for allocating future grants. Including all resources and identifying priorities could help implementing parties allocate grants according to priorities and constraints, and could help stakeholders shift such investments and resources as appropriate. Such guidance would also assist Congress and the executive branch in developing more effective programs that leverage finite resources.

Integration and Implementation

While the Freight Rail Modal Annex delineates mechanisms to facilitate stakeholder coordination, specifically the FRGCC and FRSCC, and discusses other relevant industry security plans, it does not address its relationship with strategic documents or activities of other federal agencies that have roles in freight rail security, such as those that guide DHS IP, whose responsibilities overlap with TSA's for protecting freight rail critical infrastructure.⁶⁷ For example, the annex does not mention how DHS IP's initiatives, such as the BZPP and SAV assessments of freight rail assets, fit into TSA's overall strategy. In addition, the annex does not identify how it complements, relates to, or builds upon the NSTS required by the Intelligence Reform and Terrorism Prevention Act of 2004.⁶⁸ Without such information in TSA's national strategy for freight rail security, the agency is missing opportunities to identify linkages with other developed strategies and other organizational roles and responsibilities and thus further clarify the relationships between various implementing parties, both vertically and horizontally, which, in turn, could foster more effective implementation.

⁶⁷DHS IP's mission is to lead the coordinated national effort to reduce the risk to critical infrastructures and key resources posed by acts of terrorism and strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency.

⁶⁸The NSTS, required by section 4001 of IRTPA, is a national strategy for transportation security outlining the federal government's approach—in partnership with state, local, and tribal governments and private industry—to securing the U.S. transportation system from terrorist threats and attacks.

While TSA has addressed aspects of the executive order as well as key aspects of successful national strategies, more fully addressing the characteristics discussed above and taking steps to be more consistent with the provisions in Executive Order 13416 could assist TSA in further developing and strengthening its Freight Rail Security Modal Annex. These efforts could also enhance the strategy's usefulness in resource and policy decisions to better ensure accountability by making decision making more transparent and comprehensive.

Federal Efforts Have Guided Voluntary Industry Actions and Generally Focused on TIH, but New Requirements Could Pose Challenges

Since September 11, 2001, federal and industry stakeholders have implemented a range of actions to secure the freight rail system, many of which have focused on securing TIH shipments and have been implemented by industry voluntarily. However, TSA's ability to assess the impact of various security efforts is limited because the agency lacks a mechanism to systematically track the actions being taken and evaluate their effectiveness. Furthermore, a variety of new regulations have recently been promulgated that will make some freight rail security actions mandatory. Implementing these new requirements as well as other security assessment and planning requirements stemming from the 9/11 Commission Act is expected to necessitate additional efforts and resources from both federal and industry stakeholders and may pose some implementation challenges, such as TSA's requirement for handlers of certain highly hazardous materials to implement steps to establish a secure chain of custody and control for railcars in their possession containing these materials.

TSA and DOT Actions Have Been Primarily Focused on Mitigating TIH Threats and Have Been Presented to Industry as Voluntary Measures

In keeping with TSA's strategy, since September 11, 2001, most federal actions to enhance freight rail security have focused on mitigating the risk of transporting TIH materials over the freight rail system, and most of these efforts have been proposed as voluntary measures that industry could implement. Overall, federal agencies, including TSA, FRA, and PHMSA, have worked together and with the major private industry stakeholders, such as AAR and numerous individual rail and chemical companies, both large and small, to discuss, develop, and implement TIH risk-mitigating actions. For example, TSA worked closely with individual rail companies to develop and implement various voluntary risk mitigation strategies as part of its Corridor Reviews.

TSA officials said that taking a voluntary approach allowed them to work collaboratively with industry to identify, tailor, and implement security actions in less time and with fewer resources than would have been

needed to develop and implement TIH security regulations. For example, many of TSA's recommended actions provided to rail carriers through its Corridor Reviews were developed collaboratively with each rail carrier during TSA's on-site visits and were tailored to each carrier's specific operations. In addition, TSA's and DOT's voluntary security action items also provided rail carriers flexibility in their implementation and allowed rail carriers to adopt measures best suited to their particular circumstances. TSA officials told us that this approach allowed them to more quickly address identified security gaps, especially given the TIH risk and the open nature of the rail system. Both federal and industry officials acknowledged the inherent openness and accessibility of the rail system and also told us that it is extremely challenging to completely secure the rail system because of its size and the need for railcars to be able to continuously move on tracks and in and out of rail yards. Limited resources were also a factor in determining TSA's approach to working with the freight rail industry and heavy focus on TIH shipments, according to agency officials. As a result, agency officials reported focusing much of their time to finding ways to secure TIH rail shipments through implementing operational changes that required few resources. Key federal agency security actions taken since September 11, 2001, are summarized in table 6. Additional information is provided in appendix IV.

Table 6: Key Federal Security Actions Taken since September 11, 2001

TSA Corridor Review recommendations: Through the Corridor Reviews, TSA identifies specific security actions that rail carriers can voluntarily adopt to reduce freight rail security risks involving TIH. TSA focuses its recommended actions at rail yards containing TIH, locations where TIH cars are exchanged, or other significant choke points where TIH railcars may stop and be vulnerable to tampering. TSA officials reported focusing more on recommending operational changes because they are often less costly for the railroads to implement than physical security upgrades. Generally, operational changes focus on reducing the amount of time TIH railcars remain on rail tracks or in rail yards located in major urban areas and on increasing the visibility of the cars by rail employees.

Voluntary freight rail security action items for the rail transportation of TIH: TSA and DOT issued 24 action items in June 2006, which were developed in concert with key industry stakeholders and addressed system security, access controls, and en route security.^a In November 2006, TSA and DOT issued an additional 3 action items, called supplemental security action items, which also focused on TIH rail shipments. TSA officials said that all 27 security action items were identified through the information and findings that TSA and DOT had gathered from previously conducted corridor reviews, site inspections, and security plan reviews.

TSA surface transportation security inspectors (STSI): STSIs conduct on-site inspections of U.S. rail systems working collaboratively with freight rail carriers, the mass transit and passenger rail industry, and applicable local, state, and federal authorities to identify best security practices, evaluate security system performance, and discover and correct deficiencies and vulnerabilities in the industry's security systems, including noncompliance with mandatory security requirements.^b For freight rail, STSIs have assessed the industry's implementation of 17 of the original 24 voluntary freight rail security action items, and have conducted site visits to rail yards in high-threat urban areas to assess the attended status of TIH railcars as part of TSA's TIH Rail Risk Monitoring Program.

DHS grant funding: Since 2005, DHS has awarded a total of \$7.5 million to the freight rail industry to develop a risk assessment tool intended to assist railroads in selecting safe and secure rail routes for their TIH shipments.^c In addition, in 2008, DHS established the Freight Rail Security Grant Program (FRSGP), which provided \$4.9 million in 2008 to six railroads, among other things, to provide for a training program and conduct vulnerability assessments.^d Furthermore, through the end of 2008, FEMA officials told us that they have awarded about \$4.6 million, through DHS IP's BZPP, for the purchase of security-related equipment to protect freight rail assets from terrorist attack.^e DHS IP also created the National Capital Region Rail Pilot Project, which implemented a remote intelligent video security system through the Washington, D.C., rail corridor. DHS IP, TSA, and the rail industry plan to brief and demonstrate this project in other major cities to provide stakeholders with an overview the system's capabilities, and DHS intends to provide grant funding for installing similar systems in other cities.

Source: GAO analysis of DHS, DOT, and industry data.

^aTSA and DOT coordinated with AAR and the American Short Line and Regional Railroad Association (ASLRRA) to develop the recommended security action items. System security and access control refer to practices affecting the security of the railroad and its property. En route security refers to the actual movement and handling of railcars containing TIH materials.

^bIn response to a directive in the conference report accompanying the DHS appropriations act for fiscal year 2005, TSA established the Surface Transportation Security Inspection Program. This program works to build a collaborative working relationship with freight rail carriers, the mass transit and passenger rail industry, as well as applicable local, state, and federal authorities to identify best security practices, evaluate security system performance, and discover and correct deficiencies and vulnerabilities in the industry's security systems, including noncompliance with mandatory security requirements.

^cThe Railroad Research Foundation, a not-for-profit research-oriented corporation, established in November 1999 and affiliated with AAR, has been overseeing the development of this project in coordination with federal stakeholders.

^dThe FRSGP was created under the 9/11 Commission Act and is a new component of the Transit Security Grant Program. The FRSGP defines Security Sensitive Material as more than 2,268 kilograms in a single carload of a Division 1.1, 1.2, or 1.3 explosive; a tank car containing a TIH material, as defined in 49 C.F.R. § 171.8, including anhydrous ammonia, but excluding residue quantities of these materials; and a highway route-controlled quantity of a Class 7 (radioactive) materials as defined in 49 C.F.R. § 173.403.

⁶⁸Through BZPP, DHS provides grant money, through the states, to local law enforcement agencies, including railroad police, to purchase security-related equipment to protect rail assets. Examples of items purchased include chemical protective clothing, bulletproof vests, video surveillance equipment, and portable radios. Although DHS IP is responsible for the assessment, FEMA, as the final approver of the grant, ultimately awards the grant funding to the states. However, FEMA officials told us that they capture program expenditures differently than DHS IP. As a result, FEMA could not provide specific information for roughly \$180,000 of the \$4.8 million DHS IP officials told us had been disbursed through the program to protect freight rail assets.

While Many Industry Actions Focused on Securing TIH Rail Shipments, Other Actions Addressed Non-TIH-Related Security Threats

The freight rail and chemical industries have voluntarily taken various actions to secure TIH rail shipments even beyond what TSA has recommended, and some industry actions have addressed other identified freight rail security threats.⁶⁹ For example, in addition to taking actions in response to TSA's recommendations resulting from the Corridor Reviews, some rail industry stakeholders we spoke with have implemented other types of operational and procedural changes to secure their TIH rail shipments, such as making modifications to procedures for how rail companies manage and schedule trains and railcars. These changes have largely focused on reducing the amount of time that TIH railcars remain on rail tracks or in rail yards located in major urban areas. Railroad officials we interviewed from six of the seven Class I railroads told us that they implemented these changes in response to TSA's and DOT's supplemental security action items—issued in November 2006—and to address general federal, state, and local government concerns over the secure transportation of these materials. These railroad officials also stated that they had hoped their actions would preempt future local or state restrictions attempting to force them to reroute TIH and other highly hazardous materials rail shipments on to longer, less desirable rail routes.

In addition, officials we met with from three railroads and two chemical companies stated that they had also taken steps to attempt to better track the movements of their TIH rail shipments by installing Global Positioning System technology on their locomotives and tank cars. The chemical industry is also leading an effort, in partnership with rail and federal stakeholders, to research ways to construct a rail tank car that is more resistant to rupture or breach in the event of a derailment or intentional attack. The most significant rail industry security action, however, has

⁶⁹In addition to securing their TIH rail shipments, chemical companies have also taken various other security-related actions to secure their facilities. Certain chemical facilities are also subject to the DHS's Chemical Facility Anti-Terrorism Standards Program, which requires facilities that are determined to be high risk to complete site security plans that include measures that satisfy DHS risk-based performance standards.

been the development of an industrywide security management plan. This plan, developed in 2001 by AAR in coordination with its member railroads and several chemical industry associations, did not exclusively focus on securing TIH but also addressed other threats, such as those to critical infrastructure and the security of critical railroad information. For example, the plan provides a ranking and prioritization of the industry's infrastructure that it deemed most critical, such as key bridges, tunnels, and operations centers. The plan also served as a template for individual railroads to follow in developing or modifying their own security plans. Individual rail and chemical companies have also undertaken efforts to implement various physical enhancements to their facilities, such as erecting fences and installing cameras at key rail yards, bridges, and tunnels. In addition to the security plan, AAR established the Rail Alert Network to coordinate alert-level security actions industrywide. These measures help to mitigate the risks not only from TIH, but other threats as well, for example, by helping to secure facilities and assets from destruction or sabotage, which could cause a degradation or shutdown of rail service. More information on the various security actions taken by industry since September 11, 2001, is in appendix IV.

While industry has taken a range of actions to better secure their rail networks, including making operational changes, furthering technology and research and development efforts, and implementing physical security upgrades at some facilities, industry stakeholders we met with stated that it is difficult to completely secure their networks because of the size and openness of the rail system.⁷⁰ We also observed this inherent challenge during our site visits to various rail facilities. For example, while officials we interviewed from all seven Class I railroads and six short line railroads reported installing fencing at some of their rail facilities, such as intermodal yards and key business facilities, most of the rail yards we visited during our site visits did not have fencing, and most rail carriers told us that they did not consider fencing a cost-effective security

⁷⁰For additional information on some of the specific technology challenges federal and industry stakeholders face in better securing TIH shipments, see app. V. These challenges include designing stronger tank cars, developing more real-time railcar tracking and monitoring systems, and substituting highly hazardous materials with less dangerous chemicals.

measure.⁷¹ Specifically, larger rail yards, such as rail classification or switching yards where TIH cars would likely be located, can sometimes be over a mile or more in length, making them difficult to fence. Also, rail officials said that fencing is not a particularly difficult security measure to circumvent, and that it is difficult to completely fence a rail yard since trains need to be able to routinely move in and out.⁷² As a result, we observed rail carriers relying more heavily on other types of security measures at their larger facilities, such as surveillance cameras, enhanced lighting, random security patrols, promoting the awareness and vigilance of employees, and observation towers that could be used as security lookouts. However, although many of the larger yards we visited had observation towers, these towers sometimes did not provide a clear view of the entire yard. Figure 3 shows the view from an observation tower located in a rail yard we visited that regularly holds TIH railcars.

⁷¹An intermodal freight rail yard is a yard that handles the transportation of freight in containers that can be transported by multiple modes of transportation (rail, ship, and truck), without any handling of the freight itself when changing modes. Railroads told us that these yards often handle higher value goods that may be subject greater instances of theft. As a result, railroads told us that these yards are more frequently fenced.

⁷²Most large rail yards, often called classification and switching yards, are comprised of a complex series of rail tracks for storing, sorting, or loading/unloading railroad cars, locomotives, or both. Railcars in a yard may be sorted by numerous categories, including railroad company, whether they are loaded or unloaded, destination, car type, or whether they need repairs. The purpose of railroad yards is to store cars while they are not being loaded or unloaded or are waiting to be assembled into trains. Local serving yards are often smaller yards near local customers served by the railroad.

Figure 3: View from Observation Tower at a Rail Yard



Source: GAO.

Although TSA Has Made Some Progress Measuring the Impact of Its Corridor Reviews, It Has Not Systematically Tracked or Assessed the Impact of Many Actions to Secure Freight Rail

While TSA has made some progress in measuring the degree to which rail carrier actions taken through the Corridor Reviews have reduced risks, it has not yet systematically tracked the full scope of actions being taken or assessed their impact on reducing risks. TSA recently implemented actions to determine the risk reduction achieved as a result of its recommendations made through the Corridor Reviews and subsequent railroad actions. For example, during its Chicago review in late 2007, TSA began documenting how rail carrier actions implemented at the time of TSA's Corridor Reviews have reduced risk by determining a risk score for each asset or location both before and after rail carrier actions were taken. In 2008, TSA reported that it began taking steps to follow up with rail carriers operating in some previously reviewed cities to identify any actions the carriers may have taken in response to prior Corridor Review recommendations, and to determine how those actions may have reduced risk for the corridor.⁷³

⁷³While TSA did not follow up with all rail carriers in cities it previously reviewed, it did focus its follow-up on cities that had large rail networks and large quantities of TIH rail shipments routinely traversing them.

When we accompanied TSA's officials during their site visits to rail carriers in Chicago, we observed one rail carrier that prior to TSA's review, routinely stored loaded TIH railcars in an unmanned rail yard over the weekend to be delivered to a nearby customer facility on Monday mornings. As a result, the cars sat unattended for 2 days, posing a risk to the community. However, upon TSA's on-site recommendation, the railroad agreed to immediately change its operating procedures to store the cars during weekends at a yard that is manned 24 hours a day, 7 days a week. TSA then determined the degree to which this change reduced risk for the corridor.

However, TSA has not yet fully developed a process for systematically (1) following up with rail carriers about agency recommendations to determine the full scope of actions that rail carriers may have taken as a result of the Corridor Reviews, (2) documenting these actions, and (3) assessing their impacts on risk reduction. For example, officials at one Class I railroad we interviewed reported that they made an operational change in Buffalo, New York, to address a security vulnerability— involving loaded TIH cars being left unattended in a rail yard for up to 36 hours—that TSA identified during the Corridor Review in that region. However, TSA's Buffalo Corridor Review Summary Report developed after the Buffalo review did not explain the recommended action nor did it discuss any industry actions taken or their impact on reducing risk. While TSA officials reported being able to confirm some railroad actions through informal efforts—either through direct contact with railroad officials or through feedback from its STSIs during their visits to freight rail facilities—TSA has not established a formal process for agency program officials or inspectors to follow up on and track prior agency recommendations to determine if rail carriers had implemented them. Pursuant to Executive Order 13416, TSA is tasked with evaluating the effectiveness and efficiency of current federal government surface transportation security initiatives. In addition, Standards for Internal Control in the Federal Government calls for controls to be designed to ensure that an agency has relevant and reliable information about programs and that ongoing monitoring occurs.⁷⁴

TSA officials told us that implementing a process for following up on prior agency recommendations and confirming their implementation is a task that will likely be carried out by TSA's STSIs, as part of their new Corridor Review responsibilities in 2009. Specifically, TSA officials told us that STSIs are currently being trained to conduct future reviews in cities for which they already have inspection responsibilities. However, TSA officials told us that the STSIs are to lead reviews for cities with smaller rail networks, and that TSA headquarters officials are to remain the lead in conducting future reviews for cities with larger rail networks. TSA also said that headquarters officials are to continue to be the lead in conducting all future tabletop scoring sessions at the end of the reviews, which quantitatively score the risk posed by TIH rail shipments at various rail locations within a city. However, TSA said that it will likely be the STSIs' responsibility to follow up with rail carriers to confirm the

⁷⁴GAO/AIMD-00-21.3.1.

implementation of agency recommendations resulting from the Corridor Reviews. While we believe that training the STSIs to take a more active role in future Corridor Reviews is a positive step toward better utilizing STSI local knowledge, it is too soon to know how effective the STSIs will be in this effort and in systematically determining the full scope of the actions being taken as a result of the Corridor Reviews and how those actions have reduced risk.

TSA has also not yet assessed the impact of industry efforts to address identified security risks unrelated to TIH rail shipments as required by the NIPP. For example, railroads have taken action to better secure their bridges and tunnels, operations centers, and even their fuel depots, which, for example, contain millions of gallons of diesel fuel and are critical to railroad operations. Failing to protect these critical assets could impede the transportation of goods, possibly lead to loss of life, and have an economic impact, according to several industry officials we spoke with. Industry officials also reported that efforts to harden critical infrastructure are important to help reduce risk, and that some security enhancements they implemented were funded through DHS grants. While TSA has conducted CSR visits, which provide an opportunity to review railroad critical infrastructure information included in a company's security plan, these reviews do not provide the type of detailed information necessary to ensure that specific freight rail infrastructure assets, particularly those deemed nationally critical, are protected. For example, the DHS IP has taken action to identify freight rail assets that, if destroyed or disrupted, could cause national or regional catastrophic effects. However, TSA's CSRs do not provide any specific information on the level of overall security preparedness for these assets. Developing a mechanism to track the protective security measures being implemented and assess their impact on reducing risk could strengthen TSA's ability to determine the level of overall security preparedness within the system and use this information to effectively prioritize its resources.

New Requirements Outline a Mandatory Approach for Securing Freight Rail, Which May Create Challenges for Some Stakeholders

While the majority of actions taken to secure freight rail have been taken on a voluntary basis, new TSA, PHMSA, and FRA regulations and the 9/11 Commission Act herald a new approach that sets forth mandatory requirements, which may create challenges for both federal and industry stakeholders. On November 26, 2008, TSA, PHMSA, and FRA issued new regulations to enhance the security and safety of hazardous materials transportation via rail. PHMSA's regulation describes, among other things, steps that rail carriers must take to determine the safest and most secure routing of highly hazardous materials, while FRA's regulation describes

the process the agency will follow in enforcing the PHMSA routing rule, TSA's regulation outlines steps that handlers of highly hazardous materials must take to establish a secure chain of custody and control for hazardous materials railcars in their possession. On April 1, 2008, PHMSA, in coordination with FRA, also proposed a regulation that would, if finalized, enhance safety performance standards for rail tank cars carrying certain highly hazardous materials, and on January 13, 2009, PHMSA, in coordination with FRA, issued a rule establishing interim standards for rail tank cars transporting TIH materials. TSA, PHMSA, and FRA officials with whom we spoke stated that many of the security-related requirements outlined in these rulemakings were derived from findings gathered during prior federal assessments and through federal inspections of rail carrier facilities.

TSA officials also told us that their shift from a voluntary to a more regulatory approach for securing freight rail was the result of several factors, including the need to

- clarify federal authority with respect to rail security as well as authority for conducting security inspections at rail facilities;
- preempt future state or local government efforts to regulate certain aspects of freight rail security, such as the routing of hazardous materials;
- address certain rail carrier business operating practices that routinely created security vulnerabilities, such as how TIH railcars were exchanged; and
- formalize security measures that rail carriers had already implemented voluntarily and ensure that security measures are maintained by these companies and any others that enter the market.

In addition, the 9/11 Commission Act provides a preview of other new requirements that federal and industry freight rail security stakeholders will face when these measures are implemented. Table 7 summarizes these new and proposed requirements. More detailed information on these requirements and actions is contained in appendixes IV and VI.

Table 7: Key Rulemakings and Legislative Requirements Affecting Freight Rail Security

PHMSA's rail safety and security rule: PHMSA's rule requires rail carriers, among other things, to take the following steps to enhance the safety and security of certain shipments of security-sensitive hazardous materials, including TIH: compile annual data on shipments of these materials; use the data to analyze safety and security risks along rail routes where those materials are transported; assess alternative routing options, including interchanging the traffic with other railroad carriers; seek information from state, local, and tribal officials regarding security risks to high-consequence targets along or in proximity to the routes; consider mitigation measures to reduce safety and security risks; and select the practicable routes that pose the least overall safety and security risks. FRA's enforcement rule discusses steps it may take to require a railroad to use an alternative route to the one selected by the railroad if FRA determines that the railroad's route analysis does not support the railroad's original selected route, that safety and security considerations establish a significant preference for an alternative route, and that the alternative route is commercially practicable. FRA's rule also establishes procedures to enable a railroad to challenge any rail routing decisions made by FRA.^a

PHMSA-proposed rail safety rule covering operations and tank car standards: PHMSA's proposed rail safety rule would enhance the performance standards for tank cars used to transport highly hazardous materials and implement operational restrictions to improve accident survivability and enhance the cars' resistance to rupture or puncture during a derailment. While this proposed regulation focused on safety, FRA officials we spoke with said that these enhancements would also have security benefits. Pending the completion of this rulemaking, PHMSA, in coordination with FRA, issued a rule on January 13, 2009, establishing enhanced performance standards for tank cars used to transport TIH and imposing a 50 miles per hour maximum speed restriction on all loaded TIH rail cars.^b

TSA rail security rule: TSA's rail security rule establishes general security requirements for rail entities and additional security requirements for entities dealing with certain hazardous materials, including TIH. The rule requires, among other things, certain rail carriers, shippers, and receivers to establish and provide for a secure chain of custody and control for railcars in their possession that contain the selected hazardous materials.^c

The 9/11 Commission Act: The act, signed into law on August 3, 2007, requires federal stakeholders to take several steps to further secure the freight rail system, including TIH shipments. For example, the act requires, among other things, that DHS complete a nationwide railroad risk assessment, assign each rail carrier to a tier of risk, and issue regulations requiring each carrier assigned to a high-risk tier to conduct a vulnerability assessment and implement a security plan. TSA must also establish standards and guidelines for developing and implementing these assessments and plans, and railroads assigned to a high-risk tier must submit the vulnerability assessments and security plans to TSA for approval. TSA must then review each assessment and plan, require amendments to any plan that does not meet the applicable requirements, and approve assessments and plans that meet the applicable requirements. The act also requires DHS to conduct a vulnerability assessment of railroad tank cars used to transport TIH materials and submit various progress reports to Congress.^d

Source: GAO analysis of DHS, DOT, TSA, and industry data.

^aHazardous Materials: Enhancing Rail Transportation Safety and Security for Hazardous Materials Rail Shipments, 73 Fed. Reg. 72,182 (Nov. 26, 2008); Railroad Safety Enforcement Procedures; Enforcement, Appeal and Hearing Procedures for Rail Routing Decisions, 73 Fed. Reg. 72,194 (Nov. 26, 2008).

^bHazardous Materials: Improving the Safety of Railroad Tank Car Transportation of Hazardous Materials, 73 Fed. Reg. 17,818 (Apr. 1, 2008); 74 Fed. Reg. 1770 (Jan. 13, 2009).

^cRail Transportation Security, 73 Fed. Reg. 72,130 (Nov. 26, 2008).

^dSpecifically, the act requires that the NSTS include a 3-year and a 10-year budget for federal transportation security programs that will achieve NSTS priorities, methods for linking the individual transportation modal security plans, and a plan for addressing intermodal transportation.

TSA's Rail Security Rule May Pose Challenges to Some Industry Stakeholders

Several industry stakeholders we spoke with raised concerns about TSA's requirement that certain rail carriers, shippers, and receivers of highly hazardous materials rail shipments implement operational procedures to provide for a secure transfer or chain of custody and control for these

materials. Under this new rule, certain rail shippers, carriers, and receivers must take specific actions in certain circumstances, such as ensuring that a railcar is not left unattended while waiting for a transfer of custody, which, according to industry stakeholders, will likely create challenges for some rail carriers and receivers, particularly smaller ones. Officials from smaller rail and chemical companies that may be affected by this requirement expressed concern about the cost implications for their companies.⁷⁵ For example, according to officials from smaller railroad and chemical companies, railroads typically do not run a set schedule, which can create problems in coordinating the exchanges of railcars between carriers and receivers. For those companies that do not operate on a 24-hour schedule, the interchange or delivery of TIH cars during nonworking hours, or on holidays or weekends, can be problematic, and many of the smaller railroads and chemical companies do not operate on a 24-hour schedule, according to these officials. They also reported having limited staffing resources to coordinate these exchanges. Officials we spoke with from all seven Class I rail carriers commented that difficulties coordinating the exchanges of railcars with other carriers and customers will likely create resource and operational challenges for them as well. For example, officials stated that additional railroad personnel may have to be added to stay with the railcars until the exchanges can be made, or railcars may have to be returned to a local serving yard to ensure that they are attended, and these returned cars would then likely occupy track space until they could be redelivered at another time. This in turn could slow yard operations and the network, and railroad officials commented that railcars sitting idle in yards are not usually generating revenue for them.

While industry officials with whom we spoke generally supported the secure chain of custody and control requirement in concept, officials from two Class I railroads we interviewed questioned its security benefit. Industry officials questioned the benefit in part because of the nature of railroad operations. For example, some trains can be up to a mile long, making it difficult for someone, or even a small group of people, to help secure railcars and respond to incidents. As a result, rail officials questioned whether this rule will significantly enhance the security of TIH railcars. However, TSA officials believe that loaded TIH railcars sitting unattended in highly populated areas present an unacceptable public risk.

⁷⁵TSA estimated that the 10-year cost of the regulation would range from \$152.8 million to \$173.9 million. It also stated that the regulation would have a yet-to-be-determined impact on small businesses.

Impact of PHMSA's Rule on
Hazardous Material Route
Selection Is Uncertain

Furthermore, TSA's analyses, especially those derived from early Corridor Reviews, concluded that railroads, shippers, and receivers consistently lacked positive chain of custody and control procedures for railcars as they moved through the rail system and transferred from one entity to another. TSA officials stated that they had observed unattended TIH railcars, and in some cases trains, that rail carriers had left unattended for significant periods of time while awaiting eventual pickup by another rail carrier or the customer.⁷⁶ Given the risk associated with TIH materials, TSA stated that requiring rail carriers to adopt this procedural change will mitigate this vulnerability during railcar exchanges and reduce risks to the public.

It is uncertain what the impact of PHMSA's rule on enhancing the security and safety of certain hazardous materials rail shipments will be because the rule lacks direction and guidance for how rail carriers are to apply and weigh the risk criteria for conducting the required routing analysis. As a result, it is unclear to what degree rail carriers will consistently apply these criteria in conducting their analyses and making routing decisions. Specifically, the rule includes 27 specific risk criteria, such as proximity to iconic targets and population density along the route, that rail carriers are required to consider and use when conducting their routing analyses. However, the rule does not contain any specific requirements, direction, or guidance for how rail carriers are to apply and weigh the 27 risk criteria when conducting their analyses. As a result, the impact of the required analysis and rule is uncertain, raising questions regarding how consistently the rail carriers will apply the criteria to their analyses or routing decisions to ensure that the safest and most secure rail routes are selected for their highly hazardous materials rail shipments. However, PHMSA officials stated that they rejected more prescriptive approaches to the routing analysis requirement because they believe that rail carriers are in the best position to identify and assess their systems and they expect carriers to make conscientious efforts to develop logical and defensible route selections using the criteria outlined in the rule. While PHMSA officials told us that they agree that how the criteria are weighted and used is an extremely important aspect of an overall safety and security risk assessment methodology, PHMSA officials believe that a one-size-fits-all

⁷⁶In one instance TSA observed unattended, fully loaded TIH railcars left at rail track siding for 72 hours over the weekend.

approach to weighting the criteria provides insufficient flexibility for rail carriers to address unique local conditions or concerns.⁷⁷

State and local governments and environmental groups have also raised concerns about the lack of definitive guidance in the rule on how to weigh the 27 criteria. Moreover, AAR stated that analyzing such factors as population density, venues, and proximity to iconic targets, as required under the rule, does not change the fact that railroad lines link cities and entities within some of these cities that require the delivery of some hazardous materials. As a result, the transportation of security-sensitive hazardous materials by rail will likely continue to occur on routes that pass through cities where people live and iconic targets exist regardless of the routing analysis results. For example, some chemical companies that use large amounts of TIH chemicals for their business processes are located in major cities, such as Newark, New Jersey. Also, many large rail-switching yards that break apart trains and rebuild new ones are also located in major cities. As such, many highly hazardous chemical railcars traverse major cities to either arrive at their final destinations, or are within major cities when added to trains headed to their final destinations.

New Requirements in the 9/11 Commission Act and TSA's Regulations May Create Some Implementation and Resource Challenges for TSA

The new requirements under the 9/11 Commission Act are expected to create implementation and resource challenges for some federal and industry stakeholders given the extent of the requirements and, in some case, the short time frames required for their implementation. Many of the requirements fall under DHS's purview and several deadlines for implementing them have already passed. For example, the 9/11 Commission Act required TSA to complete a national railroad risk assessment by February 2008; however, TSA does not anticipate completing this requirement until the first quarter of 2009. Moreover, the 9/11 Commission Act required TSA, by August 2008, to assign railroads to tiers of risk and issue regulations requiring each railroad carrier assigned to a high-risk tier to conduct a vulnerability assessment and then prepare, submit to the Secretary of Homeland Security for approval, and implement a security plan. However, TSA has not yet fulfilled this requirement. Officials said that because of the comprehensive scope of this and some other 9/11 Commission Act requirements, as well as the need to coordinate these actions with various entities as required by the legislation, many of

⁷⁷For example, PHMSA stated that one or more criteria may need to be weighted more strongly than they would be for other areas or localities. Alternatively, some criteria may not apply to a given area or locality. See app. IV for additional information on FRA's plans to enforce compliance with the rule.

the timetables provided in the 9/11 Commission Act have been difficult to meet. TSA officials also reported that for some of the requirements calling for TSA to develop and issue regulations, they are considering consolidating rulemakings across the freight rail, passenger rail, mass transit, and motor carrier modes, which will likely further increase the scope, complexity, and time required to complete these tasks. TSA officials told us that the scope of some of the requirements in the act and the short time frames they had in which to implement them were the primary reasons why the agency has missed some of the act's deadlines.

The requirements in TSA's rail security rule and those included in the 9/11 Commission Act may also create challenges for TSA's STSIs. Specifically, TSA program officials responsible for the STSI program as well as all three STSIs we met with during our site visits told us that their resources were already stretched thin, and new requirements for additional inspection activities would pose challenges. Although additional STSIs have been authorized and are expected to be added, given the STSIs' current responsibilities plus the future actions that may be required to enforce TSA's rule and the 9/11 Commission Act requirements for several surface transportation modes, TSA will likely face challenges prioritizing the STSIs' work to make the most efficient use of its personnel resources. For example, in addition to various freight rail security duties, STSIs' current responsibilities include carrying out various initiatives for passenger rail, such as conducting various on-site inspections of passenger rail facilities. Moreover, since 2006, TSA has significantly increased the frequency of its Visible Intermodal Protection and Response (VIPR) team operations, which the STSIs typically participate in and support.⁷⁸ STSIs have seen their participation in these operations increase, thereby decreasing the time they have available to meet freight rail security requirements. However, TSA's rail security rule is expected to add to the STSIs' duties because they will likely be tasked with ensuring the freight rail carrier and chemical industries' compliance with the new secure chain of custody and control rule. In addition, STSIs may also be responsible for performing assessments of security plans, vulnerability assessments, and training programs required under the 9/11 Commission Act. Moreover, the 9/11 Commission Act requires TSA to conduct additional assessment activities

⁷⁸In early 2006, TSA began deploying its STSIs to support VIPR deployment teams, which conduct single- or multiday security operations at various mass transit and passenger rail systems to deter and protect against potential terrorist actions. The VIPR operations represent an ongoing effort to develop surge capacity to enhance security in the transportation sectors.

on other surface modes, and TSA has reported that it plans to use its STSIs to conduct these activities as well. For example, STSIs are expected to be involved in the security reviews of the 100 most critical pipeline operators and to perform a number of highway-related activities, including documenting hazardous materials routes and tracking sensitive materials.

The 9/11 Commission Act requires DHS to employ up to 150 STSIs in fiscal year 2008, up to 175 in fiscal year 2009, and up to 200 in fiscal years 2010 and 2011. While TSA reported that it met the 9/11 Commission Act provision for hiring additional STSIs by the end of fiscal year 2008, many of its newly hired STSIs did not begin conducting field activities until early 2009, when they completed their training program. TSA also plans to dedicate a portion of its newly hired STSIs' workload to increased VIPR activities. Consequently, the additional manpower TSA plans to add to its STSI program may provide only limited relief to STSI field offices, which are already stretched thin according to some TSA officials. As a result, even with these additional resources, TSA's inspectors may face challenges in fulfilling their current and future responsibilities.

Stakeholders Have Implemented Several Strategies to Coordinate Their Efforts to Secure the Freight Rail System, but Opportunities Exist to Improve Coordination between Federal Stakeholders and Their Sector Partners

While federal and industry partners responsible for freight rail security have improved coordination by implementing several agreements that clarify roles and responsibilities, and TSA has taken steps to ensure that key stakeholders are included in coordination activities, DHS can further enhance coordination activities by leveraging the resources of its other components. In addition, both federal and industry freight rail stakeholders have improved coordination by creating and participating in various information-sharing mechanisms, but FRA and TSA have not fully coordinated on some relevant inspection activities, which could potentially result in an inefficient use of already limited stakeholder resources.

Federal and Industry Stakeholders Have Coordinated Activities and More Clearly Defined Roles and Responsibilities through Several Formal Agreements, but Coordination Challenges Remain

Multiple federal stakeholders have been working together since 2004 to define and agree on their respective roles and responsibilities for securing freight rail and have clarified their roles by establishing formal agreements; however, further coordination improvements can be made. In October 2005, we reported that agencies can strengthen their commitment to work collaboratively by articulating their agreements in formal documents, such as MOUs.⁷⁹ DHS and DOT components have negotiated three annexes to the September 2004 MOU that better define their respective roles and responsibilities for securing freight rail, and have implemented strategies to facilitate the exchange of key security data and threat information. See table 8 for an overview of the agreements into which DHS, DOT, and industry have entered.

⁷⁹See [GAO-06-15](#).

Table 8: Key Agreements Signed Involving Federal Agencies and Their Industry Partners

DHS and DOT MOU: DHS and DOT signed an MOU in September 2004, followed by three annexes that better defined department and agency roles and responsibilities regarding freight rail security, among other things, and also described how the agencies would coordinate to fulfill their respective roles. The MOU stipulated that DHS has primary responsibility for transportation security, while DOT would assist DHS with implementation of DHS's security policies.

Annex to DHS/DOT MOU related to TIH: In 2004, DHS and DOT signed the first annex, which described how each department and relevant component would implement the HSC's 2004 recommendations regarding the safe transportation of TIH materials. Specifically, this annex states that DHS and DOT will, among other things, assess the vulnerabilities of high-population areas where TIH materials are moved by rail in significant quantities and work with industry to put measures in place to mitigate identified vulnerabilities.

Annexes to DHS/DOT MOU related to TSA's coordination with FRA and PHMSA: In 2006, TSA signed two additional annexes to the MOU with FRA and PHMSA to better delineate areas of responsibility and promote coordination for hazardous materials transportation and freight rail security, respectively. Both annexes identify TSA as the lead federal agency for transportation security, including hazardous materials security. In addition, the annexes describe how TSA will coordinate with PHMSA and FRA, respectively, on certain program elements and initiatives to develop and implement a hazardous materials security strategy. Specifically, the annexes stipulate that the signatories agree to hold meetings as necessary at both headquarters and regional levels to discuss coordination of training for field inspectors, as well as coordination of inspection and enforcement actions to minimize disruption to entities being inspected and maximize inspector resources.

Dow Chemical MOC: In 2006 and 2007, Dow Chemical Company initiated the execution of three memorandums of cooperation (MOC) to facilitate the joint development of a safer, yet cost-effective rail tank car for transporting hazardous materials. Dow Chemical is the lead for this project—called the Next Generation Tank Car project—and is working on it with FRA, TSA, Transport Canada,^a Union Pacific, and Union Tank Car. According to Dow Chemical officials, the project is in the final phases of developing a prototype tank car that can withstand side impacts at four times greater speed than current tank cars, yet can hold equal volumes of material and travel under current track weight limits.^b The MOC addresses how the stakeholders are to collaborate on the tank car's design. For example, the participants agree in the MOC to provide technical assistance for, and to participate in, various research tasks, and to share data, test results, and reports produced by the research with other participants. Dow Chemical is funding 75 percent of the project, while FRA is funding the remaining 25 percent.

TSA's MOU with AAR and Railinc: In a separate collaboration effort between a federal agency and industry, TSA signed a 2007 MOU with AAR and Railinc, which stipulates that AAR and Railinc will provide industry data to TSA regarding the movements of TIH rail shipments inside major U.S. cities.^c Access to these data has allowed TSA to measure the time period that loaded TIH railcars traverse or are located within a city's boundaries. TSA has been using these data since 2007 to assist in the agency's TIH Rail Risk Monitoring Program, which we discuss later in our report.

Source: GAO analysis.

^aTransport Canada is the Canadian agency responsible for transportation safety and security.

^bCurrently, track weight limits are 286,000 pounds on most railroad main lines.

^cRailinc is a wholly owned subsidiary of AAR, and maintains industry databases, applications, and services that are embedded in the rail industry's operations and financial systems.

DHS Agencies Can Do More to Leverage Other Component Agency Resources

While TSA has taken steps to coordinate various freight rail security efforts, some DHS component agencies still face challenges in effectively leveraging other components' resources. In October 2005, we reported that by assessing their relative strengths and limitations, collaborating agencies can identify opportunities to address resource needs by leveraging each other's resources, thus obtaining additional benefits that would not be

available by working separately.⁸⁰ Under the NIPP, DHS IP has broad responsibility for coordinating critical infrastructure protection, and TSA, as the SSA for freight rail, has the lead in securing freight rail assets and systems and for developing the criteria that DHS IP uses to identify critical infrastructure for the transportation sector. However, DHS IP and the rail industry have completed much of the work assessing and securing freight rail infrastructure with little involvement from TSA. Although TSA and DHS IP coordinated their efforts for the 2006 Corridor Review and BZPP assessments in New Jersey, which resulted in some rail carriers obtaining funding under BZPP to implement some security actions in that city, TSA and DHS IP did not continue conducting these assessments collaboratively in other cities. TSA officials explained that DHS IP assessments focused on securing freight rail facilities and infrastructure while TSA Corridor Reviews focused on securing TIH rail shipments. However, some of the actions taken through DHS IP's assessments to secure freight rail yards may also have benefited the security status of TIH rail shipments being held in those yards. For example, through DHS IP's BZPP assessments in New Jersey, several railroads operating in New Jersey received funding for physical security enhancements, such as fencing and cameras, some of which were implemented at rail yards that routinely hold TIH. While TSA officials acknowledged the agency's responsibility for securing transportation infrastructure and said that they plan to develop ways to enhance freight rail infrastructure security, it is currently unclear how TSA will coordinate with DHS IP to balance this overlapping responsibility and ensure effective use of their respective resources.

TSA and DHS IP also missed opportunities to leverage industry stakeholder resources concerning information on high-priority freight rail assets by not coordinating with relevant industry stakeholders, such as AAR. For example, although AAR reported sharing its 2001 critical infrastructure list with DHS IP, AAR officials said that DHS IP did not share the list of freight rail assets included on its prioritized critical infrastructure list until 2008. According to DHS IP officials, this delay was due to their understanding that it was TSA's responsibility to share this information with industry stakeholders. Upon learning in 2008 that TSA was not doing this, DHS IP officials said that they decided to collaborate with industry stakeholders and at that time discovered that AAR's critical infrastructure list was different from its list. AAR also expressed concern that the DHS and industry lists did not agree; however, AAR officials said

⁸⁰See [GAO-06-15](#).

that they were not able to share the entire list with the federal government because of their concerns about the protection of this information as they had not yet resolved, with DHS IP, what the classification status of the AAR list would be once it is fully shared within the federal government. Additionally, the TSSP explicitly states TSA's responsibility for coordinating with the industry on identifying critical assets, and this lack of coordination between DHS and AAR affects their ability to jointly identify and agree on the most critical freight rail system assets. Establishing a coordination process to compare this information and reach consensus on the vulnerability and potential consequences associated with these assets could strengthen stakeholders' ability to effectively and efficiently enhance the security of these high-priority assets.

Stakeholders Use Several Established Mechanisms to Share Threat and Other Security-Related Information, but TSA and FRA Have Not Conducted Joint Inspections

While both federal and industry stakeholders have used several established mechanisms to share threat and other security-related information, challenges remain in coordinating other efforts, including sharing inspection data and other information. A number of mechanisms have been established to share security-related information related to freight rail, such as the National Joint Terrorism Task Force, from which several of the railroad and chemical company officials we interviewed reported receiving freight rail security-related threat information. See table 9 for more details on the information-sharing mechanisms. However, TSA officials said that there is no specific threat against the freight rail system, which has resulted in their sharing limited freight rail security-related information with stakeholders.

Despite these information-sharing mechanisms, FRA and TSA have not coordinated on sharing some key data, and TSA could better leverage FRA's resources related to information sharing. For example, TSA officials said that they do not request the data FRA collects through its rail carrier and chemical facility inspections because they believe these data are safety related and would not be useful. However, FRA officials stated that these data include deficiencies in security plans and training activities—information that could be particularly useful to TSA since the agency is currently developing a regulation to require high-risk rail carriers to develop and implement security plans and plans to continue conducting corporate security reviews of rail carriers' security plans in the future. Our past work has highlighted the need for agencies to share information regarding issues that cut across more than one agency, especially in high-

risk areas, such as homeland security.⁸¹ Therefore, by not consulting FRA's data, TSA is missing an opportunity to better target its rulemaking efforts to areas where the railroads are more deficient.

Although TSA and FRA signed an annex to the MOU in 2006 to improve coordination, in practice, TSA and FRA officials stated that coordination occurs more at the headquarters and regional levels and less at the field level. For example, both FRA and TSA field inspectors in four locations we visited told us that they do not conduct joint inspections with one another and are not regularly in contact with inspectors from the other agency. As both TSA and FRA inspectors will likely be responsible for enforcing their respective rules and conducting various other activities required under the 9/11 Commission Act, without effective coordination, they could miss opportunities to more efficiently conduct their work. However, after reviewing a draft copy of this report, FRA officials told us that they plan to conduct joint inspections with TSA in the future when FRA and TSA inspectors are fully trained on the new regulatory requirements recently issued by both PHMSA and TSA.

Federal and Industry Stakeholders Have Developed Several Formal Committees and Other Entities to Coordinate Activities, and TSA Has Taken Steps to Include Key Stakeholders in These Activities

Industry stakeholders established multiple coordinating committees that have undertaken a range of issues of mutual concern, but not all relevant stakeholders participate in these committees. On the industry side, stakeholders, through several railroad and chemical industry associations, have taken the initiative to establish committees as recommended in the NIPP that provide opportunities for representatives from multiple organizations to discuss freight rail issues and share information. For example, both AAR and ASLRRA have established committees that focus on freight rail security issues. See table 9 for a description of the various formal committees and other established entities.

⁸¹ [GAO-06-15](#).

Table 9: Formal Committees and Other Entities Established by Federal and Industry Stakeholders to Facilitate Coordination

AAR Railroad Security Task Force: AAR established this task force soon after the September 11, 2001, terrorist attacks. It comprised AAR members, including all Class I railroads; ASLRRRA; and three chemical trade associations. It was responsible for development of the 2001 AAR industrywide security management plan.

AAR Tank Car Committee (TCC): The TCC is responsible for developing and publishing mandatory specifications for the design, construction, maintenance, and safe operation of all rail tank cars used in North America. The TCC's membership includes representatives of AAR, AAR's member railroads, ASLRRRA, the Railway Association of Canada, chemical industry associations, and tank car builders and owners. The TCC has authority to review applications for construction or modification of tank cars, and approve or deny them based on their consistency with DOT regulations. However, DOT has the authority to make all final policy judgments regarding any modifications.^a

Freight Rail Government Coordinating Council (FRGCC): TSA established FRGCC^b in 2006 for federal freight rail security stakeholders to coordinate security strategies and activities; establish policies, guidelines, and standards; and develop program metrics and performance criteria.^c FRGCC's membership includes TSA, DHS, FRA, and PHMSA, as well as the U.S. Coast Guard, U.S. Customs and Border Protection, the Surface Transportation Board (STB), the Federal Bureau of Investigation, and the Department of Defense (DOD). FRGCC meets quarterly, and has met approximately six times. One current FRGCC responsibility is to compile a nationwide risk assessment of rail carriers, as required by the 9/11 Commission Act.

Freight Rail Sector Coordinating Council (FRSCC): The freight rail industry established FRSCC in 2005 as the private sector counterpart to FRGCC.^d FRSCC is a self-organized, self-run, and self-governed council led by the presidents of AAR and ASLRRRA. The council's membership consists of representatives of AAR, ASLRRRA, all Class I rail carriers, Amtrak, four regional freight rail carriers, and two passenger railroads. According to AAR, FRSCC does not hold regular meetings because its membership duplicates a preexisting railroad industry security committee, which convenes regularly to discuss freight rail coordination. As a result, FRSCC's primary function is to convene formally to discuss freight rail security issues with FRGCC. While the committees have only met once jointly, a TSA official said that additional meetings will likely occur now that both TSA's and DOT's rail security rules have been finalized.

Critical Infrastructure/Partnership Advisory Council: TSA established this council in 2006 in response to recommendations in the NIPP, and this advisory council was primarily a partnership between government and private sector CIKR owners and operators. Its purpose was to facilitate effective coordination of federal CIKR protection activities, such as planning, coordination, NIPP implementation, and operational activities, including incident response, recovery, and reconstitution. Its membership consisted of FRGCC members and representatives from AAR, ASLRRRA, and all Class I railroads. However, the council's only activity was to develop the initial 24 security action items that TSA and DOT issued to enhance freight rail security.

DHS Executive Steering Committee (ESC): DHS formed its ESC, comprising multiple federal agencies and DHS components, including DOT, the Department of Justice (DOJ), DOD, and TSA, to provide organizational oversight, guidance, and support to the DHS Freight Rail Security Program projects and pilot initiatives.^e Activities under the program are to coordinate and support broader DHS security programs and objectives and assist government policymakers in making informed decisions to oversee the development and deployment of demonstration projects that offer the potential for long-term enhancement of freight rail security. According to DHS officials, input from the executive steering committee helped DHS to oversee the development of the rail corridor risk assessment tool.^f

Section 333 conference: Industry stakeholders have used this mechanism to discuss freight rail security for the purpose of coordinating rail carrier operations and facilities to achieve a more efficient, economical, and viable rail system.^g The conference provides participants with immunity from antitrust liability for any discussions and agreements resulting from the conference that receive FRA approval. In November 2005, AAR and the American Chemistry Council (ACC) requested the first section 333 conference to discuss ways to enhance the safe and secure transport of TIH materials. According to federal and industry officials, discussions have focused on TIH routing options and have included FRA, PHMSA, STB, DOJ, TSA, and railroad industry representatives. Chemical industry representatives have been involved in separate meetings. According to federal officials, although discussions have not resulted in routing changes that would enhance TIH shipment security, the railroads have made operational changes, such as improving the efficiency of their service. Section 333 meetings were suspended pending the issuance of DOT's final rule regarding the rail routing of TIH materials.

Source: GAO analysis of DHS, DOT, and industry data.

^a49 C.F.R. § 179.4 stipulates that the AAR TCC will review all proposed changes and specifications for tank cars, and the resulting recommendations will be considered by DOT in determining appropriate action.

^bGovernment coordinating councils comprise representatives of the SSAs; other federal departments and agencies; and state, local, and tribal governments.

^cAs the SSA for freight rail security, TSA has primary responsibility for establishing formal mechanisms for coordinating on security issues, such as government coordinating councils and advisory councils, in accordance with the NIPP and TSSP.

^dAccording to AAR, FRSCC was created in March 2005; however, it was not officially recognized by DHS until August 2006.

^eThe Freight Rail Security Program is a federally funded, DHS public-private partnership dedicated to assessing policies and technologies for enhancing security throughout the freight rail industry.

^fSee app. IV for a full description of the Web-based security tool.

^g49 U.S.C. § 333 authorizes the Secretary of Transportation, at the request of one or more railroads, to convene a conference on a proposed coordination or unification project. The law also relieves participants in such a conference from liability under antitrust laws for any discussions at the conference or agreements that are reached at the conference that are entered into with the approval of the Secretary. The Secretary has delegated this authority to the FRA Administrator.

While TSA has no official role in determining the membership of industry sector coordinating councils, TSA recognized the importance of including the chemical industry in FRGCC/FRSCC discussions about freight rail security and has attempted to encourage wider representation on FRSCC. FRSCC does not include chemical trade associations or companies in its membership, and AAR stated that the council's membership should not include the chemical industry as it is a railroad customer and the sector coordinating councils should remain separate to protect information that should remain discrete. However, according to AAR, in 2008, the FRSCC and the chemical sector coordinating council created a joint task force to address matters related to the security of hazardous materials transportation by rail. A chemical industry trade association representative has expressed an interest in being included in FRSCC's membership, stating that not allowing the chemical companies to participate in FRSCC limits their opportunities to discuss legitimate security concerns with freight rail companies. TSA invited representatives of rail shipper organizations, such as chemical trade associations, to serve as subject matter experts at the first joint meeting between the two councils in September 2007.⁸² While the NIPP requires sector coordinating council membership to be representative of a broad base of owners, operators, associations, and other entities within a sector, the sector coordinating councils are organized and run by the private sector.

⁸²FRSCC and the chemical sector coordinating council have not held a joint meeting since September 2007.

In addition to establishing formal coordination mechanisms, DHS and DOT reported that they frequently coordinate informally with various industry and federal partners. For example, both TSA and DOT officials said that they have communicated informally by phone or e-mail several times a month as issues arose, and that they coordinated in developing their respective rail security rulemakings. Moreover, TSA officials reported that they have also coordinated informally with industry on several matters. For example, TSA reported coordinating with rail carriers on-site during rail facility inspections and during Corridor Review assessments to determine actions that rail carriers could implement to address identified vulnerabilities. In addition, TSA officials said that they coordinated with rail carriers to schedule and conduct agency reviews of rail carrier corporate security plans and procedures. Finally, TSA officials said that they often communicated informally with AAR through unscheduled phone calls to discuss relevant issues, and that they often received briefings from AAR on various industry activities.

Conclusions

Because of its vast size and openness, securing the nation's freight rail network is a monumental task that requires a coordinated effort by numerous stakeholders, and we commend TSA for the efforts it has undertaken to address this security challenge. TSA's strategy for securing freight rail by reducing threats to TIH shipments has been a reasonable initial approach when considering the serious public harm that TIH materials potentially pose to the public, the results of early assessments, and the freight rail security program's limited resources. However, given the importance of the U.S. freight rail system to the national economy, the potential for other rail security risks to be exploited, and the new broadening legislative and regulatory requirements, TSA should expand its focus to threats beyond TIH. This effort should include developing estimates of the likelihood of various threats occurring to the freight rail system. In addition, while TSA's 2007 Freight Rail Modal Annex represents a positive step toward better conveying TSA's strategy for securing the freight rail mode, it lacks important details needed to provide all stakeholders with a clear and measurable path forward. The inclusion of clearly defined stakeholder roles and responsibilities could be useful to agencies and other stakeholders in fostering coordination and in helping to ensure that certain roles are carried out, particularly where responsibilities overlap. Additionally, the weakness of one performance measure and the lack of targets for the others identified in the annex inhibit TSA's and others' ability to evaluate their progress in achieving the strategy's vision. The weakness in TSA's performance measure for reporting TIH risk reduction is of particular concern. While we recognize

TSA's constructive efforts to develop its 2005 baseline data, we have concerns about data reliability and inconsistency in how TSA measured its risk reduction results. Since 2007, however, TSA has been able to collect the necessary data and has used them to develop a better approach—with a more consistent methodology—for measuring its progress and reporting results. We believe that TSA, the public, and Congress would be better informed if, going forward, TSA were to use this new approach with the 2007 data serving as its baseline measure. Although this limits TSA's ability to report on early actions taken to secure freight rail, under the new approach TSA could set new targets and have better assurance that the agency is more accurately measuring future progress in reducing TIH risks. Also, the lack of specific time frames in the annex for program completion hinders accountability by not clearly setting expectations for when security gaps should be addressed. Ensuring that the updated annex includes information on its development, including the entities that contributed to its development and the methodology they used, could also strengthen it and make it more useful to interested parties.

In addition, TSA has not systematically tracked the various actions taken to secure freight rail, nor has it assessed the degree to which those actions have mitigated identified security risks. Developing a mechanism to track these actions and assess their impact on risk could strengthen TSA's ability to determine the level of overall security preparedness within the system and to use this information to effectively prioritize its resources. Additionally, TSA and industry's efforts thus far in voluntarily working together to secure freight rail in the absence of significant federal rail security regulations have been noteworthy. Although they did not initially include all relevant stakeholders, TSA's Corridor Reviews were a positive step toward enhancing awareness of the specific risks that TIH rail shipments posed in major cities. These reviews also strengthened relationships among rail stakeholders and resulted in industry actions that helped to secure TIH shipments. However, a significant transition lies ahead. The implementation of new federal requirements will alter the current approach for securing freight rail from a voluntary to a more regulatory approach, and it will be important for both TSA and industry stakeholders to manage this transition successfully. We also recognize the inherent challenge of securing nonfixed assets, such as TIH rail cars, as they travel throughout the United States. However, the implementation of new federal requirements will present new challenges for both TSA and industry stakeholders. To meet these challenges, it will be important for TSA to engage federal and industry partners in ensuring that the actions taken to secure freight rail are both effectively and efficiently targeted toward risk reduction.

Finally, since multiple stakeholders share responsibility for securing freight rail, differences in missions, cultures, and established ways of doing business can impede coordination. The involvement of numerous stakeholders in securing freight rail highlights the importance of federal agencies working together to facilitate appropriate access to relevant information and resources to ensure efficiency and avoid duplication of efforts. While coordination efforts thus far have been generally positive, establishing a coordination process to ensure that all relevant threat, vulnerability, and consequence assessments are shared and field inspector resources are fully leveraged could strengthen the federal government's ability to ensure the security of freight rail. Given the additional responsibilities under the 9/11 Commission Act and new regulations, federal and industry cooperative efforts remain important.

Recommendations for Executive Action

To ensure that the federal government's strategy for securing the U.S. freight rail system fully addresses factors in Executive Order 13416 and contains characteristics we identified as key to successful national strategies, and to better ensure that TSA is able to successfully prioritize its resources and assess the progress of federal and industry efforts to secure the freight rail system from acts of terrorism, we are recommending that DHS's Assistant Secretary for the Transportation Security Administration take the following five actions:

- To ensure that the federal strategy to secure the freight rail system is comprehensive and considers a wider range of risk information, develop a plan for addressing identified security threats to freight rail other than TIH, such as destruction of or sabotage to freight rail bridges and tunnels and cyberattacks to the rail system, and incorporate this information and other related strategic updates into TSA's Freight Rail Modal Annex. As part of this effort, further evaluate methods for estimating the likelihood of various threats occurring and ensure that this information is also considered when developing future risk assessments and strategic updates.
- To better ensure that relevant federal and industry partners effectively leverage their resources to achieve the strategic vision of TSA's Freight Rail Modal Annex, ensure that future updates to TSA's annex more comprehensively address factors contained in Executive Order 13416 and identified key characteristics of a successful national strategy, including
 - describing the methodology used to develop the strategy and which organizations and entities contributed to its development;
 - more clearly defining federal and industry roles and responsibilities;

-
- ensuring that performance measures have defined targets and are linked to fulfilling goals and objectives;
 - more systematically addressing specific milestones for completing activities and measuring progress toward meeting identified goals;
 - more thoroughly identifying the resources and investments required to implement the strategy, including priorities for allocating future grants; and
 - more comprehensively identifying linkages with other developed strategies, such as those that guide DHS IP, whose responsibilities overlap with TSA for protecting freight rail critical infrastructure.
- To ensure that TSA is consistently and accurately measuring agency and industry performance in reducing the risk associated with TIH rail shipments in major cities, take steps to revise the baseline year associated with its TIH risk reduction performance measure to enable the agency to more accurately report results for this measure.
 - To ensure that TSA is able to more effectively assess the progress being made in securing freight rail, balance future activities against the various security risks to freight rail, and use its and industry's resources in the most cost-effective manner, take steps to more fully track and assess the implementation and effectiveness of security actions being taken to secure freight rail.
 - To better ensure that federal agencies are coordinating as effectively as possible, work with federal partners, such as DHS IP and FRA, to ensure that all relevant assessments and information are shared and TSA and FRA field inspector resources are fully leveraged.

Agency Comments and Our Evaluation

We provided a draft of this report to DHS, DOT, and DOD on February 23, 2009, for review and comment. DOD did not provide comments, and DOT provided technical comments that we incorporated as appropriate. DHS provided written comments on April 7, 2009, which are reprinted in appendix VII. In commenting on the report, DHS reported that it concurred with all five recommendations and discussed actions it has taken or planned to take to implement them. However, the actions DHS reported taking or planned to take, while relevant, do not fully address the intent of two of the five recommendations. DHS also provided summary information on freight rail security actions that it has taken in recent months or intends to take in the future.

With regard to our first recommendation that TSA develop a plan for addressing identified security threats to freight rail other than TIH and further evaluate methods for estimating the likelihood of various threats

occurring, DHS stated that it concurred with the recommendation. DHS also reported that it is currently developing an initiative to address the security of critical railroad infrastructure and to assist in this effort has developed a draft tool designed to measure the criticality and vulnerability of freight rail infrastructure. DHS added that it is coordinating this effort with and collecting input from freight rail industry stakeholders, which will be further developed through future updates to TSA's freight rail security strategy. We support TSA's efforts to expand its strategy beyond TIH by beginning to address the security of critical railroad infrastructure; however, these actions alone will not fully address the intent of our recommendation. We believe it is also important for TSA to address additional identified security threats in future updates to its strategy, such as cyberattacks to the rail system, and to further evaluate methods for estimating the likelihood of various identified security threats occurring. Without taking steps to more fully address other identified security threats, TSA cannot ensure a comprehensive freight rail security strategy moving forward, and finding ways to better estimate the actual likelihood of various freight rail security threats occurring, as directed by the NIPP, could help TSA better assess overall risks to freight assets and to the system.

With regard to our second recommendation that TSA ensure that future updates to its Freight Rail Modal Annex more comprehensively address factors contained in Executive Order 13416 and those identified as key characteristics of a successful national strategy, DHS stated that it concurred with the recommendation. DHS also stated that it endorses the elements detailed in the recommendation and will incorporate them into future updates of its Freight Rail Modal Annex, which will be designed to more specifically address elements such as stakeholder roles and linkages, goal-oriented milestones, performance measures, and future resource requirements. We believe that incorporating these elements into DHS's updates of its Freight Rail Modal Annex will enhance its usefulness in resource and policy decisions and better ensure accountability by making decision making more transparent and comprehensive.

With regard to our third recommendation that TSA take steps to revise the baseline year associated with its TIH risk reduction performance measure to ensure that the agency is consistently and accurately measuring its and industry performance in reducing the risk associated with TIH rail shipments in major cities, DHS stated that it concurred with the recommendation. DHS also reported that TSA recognizes the importance of establishing outcome-based performance measures and will establish a new 12-month baseline with empirical and quantified data, and that

current year performance will be compared to the new baseline period and scored to determine variance from year to year. Additionally, in an effort to maintain consistency, and to discern the effectiveness of the voluntary security action items, DHS stated that TSA will also continue to measure and score current performance and compare it to the original baseline year (the 12-month period preceding the adoption of the security action items from June 2005 through May 2006), but in doing so will provide sufficient information regarding possible data limitations. We recognize TSA's interest in capturing early efforts by agency and industry officials to secure TIH within the freight rail system and agree that given the potential limitations in these data and the resulting differences in how results are calculated from this initial baseline year compared to subsequent year calculations, that discussions of data limitations would be helpful. This type of disclosure would help to avoid potential confusion that could result from TSA using this additional measure, if TSA reports this measure externally. Such action would also be consistent with best practices in performance reporting.


With regard to our fourth recommendation that TSA take steps to more fully track and assess the implementation and effectiveness of actions being taken to secure freight rail, DHS stated that it concurred with the recommendation. Specifically, DHS stated that TSA will continue to track industry adoption and implementation of the security action items and plans to gain additional perspective by measuring annual TIH risk reduction performance against the previous year to determine the efficacy of freight rail initiatives and actions as they are being implemented. In addition, DHS said that TSA's Corporate Security Reviews will also provide insights into improvements that freight railroads have implemented. While we support TSA's ongoing efforts to assess progress in reducing TIH risks in high-threat urban areas, these actions will not fully address the intent of our recommendation. We believe it is important for TSA to also assess the implementation and effectiveness of security actions resulting from its individual programs, such as the Corridor Reviews, which will allow the agency to better weigh the benefits and costs of the various programs that have been implemented to secure freight rail. Specifically, TSA should, for example, ensure that its and industry's efforts to develop and implement specific security actions through the Corridor Reviews be fully documented in TSA Corridor Review reports, which the agency has begun to do recently. Furthermore, while TSA's Corporate Security Reviews provide valuable insights into security improvements being implemented by freight railroad carriers, these reviews currently do not provide the type of detailed information necessary to ensure that specific freight rail assets, particularly those on

DHS IP's prioritized critical infrastructure list, are effectively protected. As such, we believe that tracking the specific security measures being implemented for these high-priority freight rail assets is an important factor in determining the overall level of security preparedness within the system and should be addressed in future Corporate Security Reviews or other related efforts.

With regard to our fifth recommendation that TSA more closely work with federal partners, such as DHS-IP and FRA, to ensure that all relevant assessments and information are shared and that TSA and FRA field inspector resources are fully leveraged, DHS concurred with the recommendation and said that the government coordination process continues to mature and develop and that it recognizes the importance of having and maintaining strong working relationships with other government agencies. DHS also stated that it recognizes the need to specifically define roles and responsibilities with all freight rail security stakeholders, including industry and federal, state, local, and tribal governments, and will use the Freight Rail Modal Annex to define specific stakeholder roles and responsibilities. In addition, FRA told us in its technical comments that it plans to conduct joint inspections with TSA in the future when FRA and TSA inspectors are fully trained on the new regulatory requirements recently issued by both PHMSA and TSA. We support TSA, DHS IP, and FRA efforts to better coordinate relevant information and inspector resources and better define stakeholder roles and responsibilities and believe that these efforts will help to ensure that relevant assessments and information are shared among key federal freight rail security stakeholders, TSA and FRA field inspector resources are fully leveraged, and specific stakeholder roles and responsibilities are better defined.

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

If you or your staff members have any questions about this report, please contact me at (202) 512-3404 or berrickc@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix VIII.

A handwritten signature in black ink that reads "Cathleen A. Berrick". The signature is written in a cursive style with a large initial 'C' and a small 'A'.

Cathleen A. Berrick
Managing Director
Homeland Security and Justice

Appendix I: Objectives, Scope, and Methodology

Objectives

To assess the status of federal and industry efforts to secure the freight rail system, we addressed the following questions: (1) To what extent have federal and industry freight rail stakeholders assessed the risks to the nation's freight rail network, and has the Transportation Security Administration (TSA) developed a risk-based strategy—consistent with applicable federal guidance and characteristics of a successful national strategy—for securing the system? (2) What actions have federal and industry stakeholders taken to secure freight rail systems since September 11, 2001; to what extent has TSA monitored their status and effectiveness; and what, if any, challenges hinder the implementation of future actions? (3) To what extent have federal and industry stakeholders coordinated their efforts to secure the freight rail system?

Scope and Methodology

To collectively address all three questions, we reviewed freight rail security-related laws, regulations, and executive directives. We also reviewed reports on topics related to freight rail security that were previously issued by us, the Congressional Research Service, and federal and freight rail industry stakeholders. In addition, we reviewed reports we previously issued on government management requirements, best practices, and internal controls. We interviewed freight rail security stakeholders from federal, state, and local governments, as well as representatives from the freight rail industry. A complete list of the agencies and organizations visited and contacted are in table 10. Below the table, we outline the specific steps taken to answer each objective.

Appendix I: Objectives, Scope, and Methodology

Table 10: Names and Locations of Organizations Contacted

Federal agencies

Department of Homeland Security	<ul style="list-style-type: none"> • Transportation Security Administration, including the Office of Intelligence; Freight Rail Transportation Sector Network Management office; Surface Transportation Security Inspector Program officials in Washington, D.C.; and surface transportation security inspectors in New Orleans, Chicago, New Jersey, and Houston • Office of Infrastructure Protection, Washington, D.C. • Homeland Infrastructure Threat and Risk Analysis Center, Washington, D.C. • Federal Emergency Management Agency Grants Programs Directorate, Washington, D.C.
Department of Transportation	<ul style="list-style-type: none"> • Federal Railroad Administration in Washington, D.C. (including the Office of Safety Assurance and Compliance, Hazardous Materials Division, Office of Chief Counsel, and Federal Railroad Administration field inspectors in Newark, New Jersey, and Chicago) • Pipeline and Hazardous Materials Safety Administration, Office of Hazardous Materials Standards, Washington, D.C. • Surface Transportation Board, Washington, D.C.

State and local government

- National Association of Counties, Washington, D.C.
- National Conference of State Legislators, Washington, D.C.
- New Jersey Office of Homeland Security and Preparedness, Hamilton, New Jersey

Private sector

Railroad industry groups	<ul style="list-style-type: none"> • Association of American Railroads, Washington, D.C. • American Short Line and Regional Railroad Association, Washington, D.C. • Railroad Research Foundation, Washington, D.C.
Railroads	<ul style="list-style-type: none"> • Burlington Northern Santa Fe Railroad Company, Houston, Texas • Canadian National Railroad, Baton Rouge, Louisiana • Canadian Pacific Railroad, Chicago, Illinois • Conrail Shared Assets, Newark, New Jersey • CSX Railroad, Baltimore, Maryland • East Jersey Railroad Company, Bayonne, New Jersey • Kansas City Southern Railway Company, Baton Rouge, Louisiana • Morristown & Erie Railway, Morristown, New Jersey • New Orleans and Gulf Coast Railway, Westwego, Louisiana • New Orleans Public Belt Railroad, New Orleans, Louisiana • New York New Jersey Railroad, West Seneca, New York • Norfolk Southern Corporation, Atlanta, Georgia • Port Terminal Railroad Association, Houston, Texas • Union Pacific Railroad, Spring, Texas
Chemical company industry groups	<ul style="list-style-type: none"> • American Chemistry Council, Arlington, Virginia • The Chlorine Institute, Arlington, Virginia • The Fertilizer Institute, Washington, D.C.

Chemical companies	<ul style="list-style-type: none">• BASF Corporation, Florham Park, New Jersey• Dow Chemical Company, Freeport, Texas• Lyondell Chemical Company, Houston, Texas• Monsanto Chemical Company, Luling, Louisiana• Occidental Chemical Corporation, LaPorte, Texas• PPG Industries, Inc., Lake Charles, Louisiana
Other stakeholders	<ul style="list-style-type: none">• Aon Risk Services, insurance broker, Baltimore, Maryland• Union Tank Car Company, tank car manufacturer

Source: GAO.

Objective I – Freight Rail Assessments of Risk and TSA’s Security Strategy

To determine the extent to which the federal government and industry freight rail stakeholders assessed risks to the freight rail network, we analyzed federal and industry assessments to determine the nature and severity of the threats, vulnerabilities, and consequences of potential attacks to the freight rail system. Specifically, we analyzed federal security assessments that addressed components of risk (threat, vulnerability, and consequence) from the Department of Transportation (DOT), TSA, and the Department of Homeland Security (DHS) Office of Infrastructure Protection (IP). Although DHS, DOT, and industry characterized these assessments as threat, vulnerability, and consequence assessments, we did not evaluate the quality of the assessments nor did we determine the extent to which the assessments were conducted consistent with requirements outlined in the DHS National Infrastructure Protection Plan (NIPP) as this analysis was outside the scope of our work. However, we did discuss the assessments’ reported results with the respective agencies and private entities that conducted them to ascertain the efforts that were made to identify potential threats, vulnerabilities, and consequences associated with an attack on the freight rail system. Since TSA identified the rail transportation of Toxic Inhalation Hazard (TIH) materials as the highest risk to the freight rail system, we focused our effort on understanding the vulnerabilities and consequences associated with this threat. We participated in TSA’s rail Corridor Review risk assessment in Chicago to better understand the corridor review assessment process, which TSA officials told us was their key action to strengthen rail security. We also reviewed the 2001 industrywide risk assessment developed by the Association of American Railroads (AAR) and other freight rail industry stakeholders. Further, we discussed the findings of federal and industry assessments with the respective agencies and private entities responsible for them.

To determine the extent to which TSA’s strategy to secure freight rail was risk based, we identified TSA’s strategic planning document—the Freight

Rail Modal Annex to the Transportation Sector-Specific Plan (TSSP) issued in May 2007—and evaluated the extent to which this document was consistent with federal guidelines for a risk-based security strategy. Specifically, to determine the extent to which TSA’s strategy conformed to requirements and best practices, we reviewed relevant statutory requirements of the Government Performance and Results Act of 1993 (GPRA) that included general requirements to establish government strategies and programs, and the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act), which included more specific requirements for establishing a security strategy. We reviewed executive directives, including Homeland Security Presidential Directives 1, 7, and 8 and Executive Order 13416, Strengthening Surface Transportation Security. We also reviewed documents to determine the best practices for effectively implementing a risk management framework and, in particular, risk assessment best practices. Specifically, we reviewed documents, such as the NIPP and TSSP. We also compared the Freight Rail Modal Annex to our guidance on six desirable characteristics of an effective national strategy.¹ We reviewed other security strategy–related documents, such as a railroad security memorandum of understanding annex signed by both DHS and DOT that agreed to implement a work plan developed by the Homeland Security Council (HSC) in 2004.

We also reviewed TSA’s four metrics as presented in the annex and gathered detailed information from TSA on its methodology and data used to calculate its metric to reduce the risk associated with the transportation of TIH in major cities by 50 percent by the end of 2008. TSA provided us aggregated baseline data from June 1, 2005, to December 31, 2005, prior to the implementation of the TIH Rail Risk Reduction Program and a second set of results for April 1, 2008, to June 30, 2008, after its implementation for 46 TIH high-risk cities.² We met with TSA officials to understand their process and methodology for developing this measure and the data they collected. We also collected copies of completed inspection report sheets

¹GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, [GAO-04-408T](#) (Washington, D.C.: Feb. 3, 2004).

²TSA’s TIH Rail Risk Reduction Program, which began in 2007, is a transportation security assessment in 46 major urban areas that uses industry data about TIH railcar movements inside the urban area. TSA also audits the security status of the cars while at rail yards, and assesses potential consequences associated with the surrounding population. As part of this program, TSA surface transportation security inspectors conduct site visits to rail yards in high-threat urban areas to assess whether TIH railcars are under surveillance.

that TSA used to determine the relative security of TIH cars that were sampled to develop a risk score for each city. Also, we interviewed the private company that tracks the flow of railcars through cities about the reliability of its tracking devices. We discussed our concern with TSA's methodology earlier in this report.

To obtain views of the federal government's current and future state of freight rail security strategic planning, we interviewed officials from relevant federal agencies to discuss the scope and methodologies of their risk assessments and their views of the identified risks. Specifically, we determined that TSA's Transportation Security Network Management (TSNM) office was responsible for implementing the freight rail security strategy. We then discussed the office's current and future efforts with respect to strategic planning and freight rail security assessments with TSNM officials. We also discussed other federal components' efforts to assess security risks to freight rail, including the Pipeline and Hazardous Materials Safety Administration's (PHMSA) vulnerability assessment with PHMSA officials to understand the scope, methodology, and results of their report. We discussed the Tier 2 list and the policies and procedures for administering and conducting the Buffer Zone Protection Program (BZPP) and Site Assistance Visit (SAV) assessments with DHS IP officials responsible for developing these programs. We discussed freight rail threats with TSA's Office of Intelligence. We asked officials from the TSNM office for freight rail security how, if at all, they used completed assessments to develop their freight rail security strategy. We also interviewed a former executive official from the HSC who was familiar with HSC events during 2004 that affected freight rail security. We discussed with him the actions leading up to the HSC's request that DHS and DOT identify and mitigate the security risks associated with the transportation of TIH.

In addition, we interviewed numerous industry representatives to discuss their opinions of the threats, vulnerabilities, and consequences associated with freight rail and the assessments conducted to identify and mitigate those risks. Specifically, we spoke with officials from all 7 Class I railroads, which represent about 93 percent of railroad freight revenue and 67 percent of the total U.S. rail mileage. According to DHS, DOT, and AAR officials we spoke with, these railroads collectively operate in most major cities in the United States where rail service is provided and have robust security plans in place. We also interviewed officials from 7 short line and regional railroads that operated in the same cities in which we conducted site visits, with a particular focus on those railroads that had participated in a prior TSA Corridor Review and carried TIH materials. Because we

selected a nonprobability sample of short line and regional railroads, the results from our visits cannot be generalized to the entire population of over 500 railroads; however, we believe that obtaining information from these 7 railroads allowed us to better understand the views and unique operational challenges that short line and regional railroads face in the context of freight rail security. We also met with officials from the American Short Line and Regional Railroad Association (ASLRRA) to better understand short line and regional railroad operations. Further, we interviewed officials from six chemical companies that use rail services to ship TIH and other hazardous materials. We selected these companies based on their geographic proximity to the cities we conducted site visits in, and recommendations from chemical industry officials at the American Chemistry Council (ACC). Furthermore, two of the chemical companies we spoke with, Dow Chemical and BASF, are two of the largest in the world, according to several chemical industry officials we spoke with. We developed a data collection instrument to collect uniform information from the railroads and the chemical companies whose officials we interviewed and to characterize summarily these entities' views on the current and future state of freight rail security. While the results from these visits cannot be generalized to the entire population, we believe the results from these visits provided us with a broad perspective of the types of actions taken to secure freight rail and the challenges operators face in doing so.

Objective II – Key Actions Taken and Challenges

To identify the key actions federal and industry stakeholders have taken or planned to mitigate identified risks, we reviewed TSA's Freight Rail Modal Annex and discussed the rail security actions outlined in the annex with several officials from DHS components, including TSA's TSNM office for freight rail; TSA's Office of Security Operations, the Surface Transportation Security Inspectors Program Office; the National Protection and Programs Directorate (NPPD)'s DHS IP; and the Federal Emergency Management Agency's (FEMA) Grants Programs Directorate. We also met with officials from DOT's Federal Railroad Administration (FRA) and PHMSA. During these reviews, we gathered information on several freight rail security initiatives, including TSA's Corridor Reviews, 27 joint TSA and DOT voluntary security action items, DHS IP's BZPP and SAVs, and DHS FEMA grant funding for freight rail security. We also reviewed PHMSA's and TSA's rulemakings on freight rail security (Notices of Proposed Rulemaking issued in December 2006, PHMSA's interim final rule issued in April 2008, and final rules issued by both agencies in November 2008) and PHMSA's rulemakings on enhanced performance standards for rail hazardous materials tank cars (Notice of Proposed

Rulemaking issued in April 2008, and final rule for TIH tank cars issued in January 2009). We also interviewed freight rail industry stakeholders, including representatives of major freight rail industry associations and select rail and chemical companies, to determine the actions they have taken to secure their facilities, operations, and shipments. We also reviewed AAR's rail security management plan, which was identified as the prominent action taken by the freight rail industry since September 11, 2001, to secure freight rail and is a template for most railroad security plans in the United States.

To observe actions taken to secure the freight rail system and to obtain the views of railroad and chemical company representatives, as well as federal field inspector officials, we conducted site visits to seven major cities. We chose these cities based on several factors, including that the cities have been the subject of or are expected to be the subject of a TSA Corridor Review and have rail networks that typically transport significant amounts of TIH materials. To determine the U.S. cities transporting the highest amounts of TIH materials by rail, we obtained a 3-month sample of rail industry information from TSA regarding the number TIH shipments traversing major cities for the year 2007. We compared the ranking of cities based on this information with aggregate data of the quantities of TIH being transported for the year 2000. We found the relative rankings of the major cities to be similar and selected cities that appeared high on these lists. We also solicited input from AAR on the appropriateness of the cities we selected to visit. During our site visits, we met with officials from all seven Class I railroads, seven short line and regional railroads, and six chemical companies in these cities because they carry, ship, or handle TIH materials over the rail system. We used a data collection instrument to collect uniform information from these entities on the actions taken to secure freight rail. We also met with federal government officials who work in the field, including TSA surface transportation security inspectors (STSI) at four locations and FRA officials at two locations we visited. As discussed earlier in this report, while the results from our visits cannot be generalized to the entire population of railroads, chemical facilities, and industry stakeholders, we believe that the observations obtained from these visits provided us with a greater understanding of the industry's operations and perspectives.

To determine the extent to which TSA monitored the status and effectiveness of its programs, including how well the industry was complying with voluntary action items, we interviewed TSA officials responsible for these programs and reviewed available agency documentation on both federal and industry action taken to secure freight

rail. Further, we reviewed GPRA program performance standards and GAO's Standards for Internal Control in the Federal Government to further assist us in evaluating TSA's efforts to monitor and evaluate the effectiveness of actions taken.³

To identify freight rail security challenges, we solicited information from federal, state, and local freight rail security stakeholders as well as industry stakeholders on pending and new freight rail security requirements. For instance, we reviewed the rail security requirements promulgated in the 9/11 Commission Act, and discussed any implementation and resource challenges associated with the act as well as TSA's and PHMSA's security rulemakings issued in 2008. In addition, we reviewed and analyzed over 100 public stakeholder comments to TSA's and PHMSA's notices of proposed rulemakings published in December 2006. These comments were from a wide range of organizations, including federal entities, several state and city organizations, industry associations, and individual rail and chemical companies. After reviewing the comments, we interviewed stakeholders that noted important challenges to implementing these new rules. We also solicited the opinion of other stakeholder parties about the challenges in securing freight rail transportation, including state and local government representatives and representatives from advocacy groups we identified through interviews or literature searches. We attended a session of the National Conference of State Legislatures' transportation committee to discuss the risk posed by transporting TIH by rail and other types of freight rail transportation and its effect on state governments. In addition, we interviewed representatives of the National Association of Counties to obtain similar views of TIH transportation risk and its effect on local governments.

Objective III – The Extent to Which Federal and Industry Actions Are Coordinated and Challenges to Be Addressed

To determine the extent to which federal and industry stakeholders have coordinated their actions, we reviewed relevant requirements in laws and regulations and best practices. We analyzed federal and industry cooperative agreements, including DHS and DOT memorandums of understanding and freight rail industry and government memorandums of cooperation. In addition, we analyzed the public comments to TSA and PHMSA proposed rulemakings to determine the efforts that agencies made to coordinate their respective proposed rules. For PHMSA's interim final

³GAO, *Standards for Internal Control in the Federal Government*, [GAO/AIMD-00-21.3.1](#) (Washington, D.C.: November 1999).

freight rail security rule, we reviewed the government's responses to stakeholders' comments to the rule. We also assessed federal coordination efforts using criteria we developed for effective collaboration between federal agencies as well as guidance established in the NIPP for effective collaboration with industry stakeholders.⁴ To determine the mechanisms that freight rail stakeholders use to coordinate and share information, we reviewed information provided by federal agencies, such as TSA's Freight Rail Modal Annex to the TSSP, information prepared by FRA, and documentation provided to us from industry stakeholders such as AAR and ACC. To obtain information about federal actions taken to coordinate through the Freight Rail Government Coordinating Council, we talked with four of its members, including officials from the TSA TSNM office for freight rail, which heads the council. To obtain information about the nature, scope, and effectiveness of the Freight Rail Sector Coordinating Council, we talked with officials representing the council chair—AAR—and discussed the extent to which the council had been used to coordinate with the federal government. To further obtain stakeholders' opinions on federal and industry cooperation, we met with DHS, TSA, and DOT officials responsible for various freight rail security-related programs and met with relevant representatives from the freight rail and chemical industry associations. During our site visits, we also met with federal inspectors and railroad industry representatives to discuss their specific efforts to coordinate.

We conducted this performance audit from February 2007 through April 2009 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

⁴GAO, *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, [GAO-06-15](#) (Washington, D.C.: Oct. 21, 2005).

Appendix II: Federal and Industry Freight Rail Security Vulnerability and Consequence Assessment Activities Conducted since 2001

The federal government and freight rail industry stakeholders have conducted a number of threat, vulnerability, and consequence assessments since 2001. Although DHS, DOT, and industry characterized these assessments as threat, vulnerability, and consequence assessments, we did not evaluate the quality of the assessments nor did we determine the extent to which the assessments were conducted consistent with requirements outlined in the NIPP as this analysis was outside the scope of our work. However, we did discuss the assessments' reported results with the agencies and private entities that conducted them to ascertain the efforts that were made to identify potential threats, vulnerabilities, and consequences associated with an attack on the freight rail system. While these assessments were wide-ranging, special attention was given to determining the security risks associated with the transportation of TIH materials. Below is a summary of these assessments, categorized by those activities that focused exclusively on TIH risks and those that included or focused on other risks.

Assessments That Focused Exclusively on TIH Risks

PHMSA TIH Summary Report

PHMSA conducted the first federal security assessment of TIH in 2003, called the TIH Summary Report, at the request of the HSC. The study analyzed the transportation of 13 TIH materials to determine their vulnerabilities and potential consequences in the rail transportation system along with other modes of transportation, such as maritime and highway modes. PHMSA chose to focus on these 13 materials because of their high toxicity and the large volumes transported. Specifically, the report identified 3 TIH materials—chlorine, anhydrous ammonia, and ethylene oxide—that accounted for 90 percent of the total volume shipped via rail.

TSA Rail Corridor Reviews

In 2004, TSA began conducting Corridor Reviews, which are detailed freight rail security assessments that focus on TIH rail shipments in individual cities. They are conducted by teams of TSA subject matter experts and are designed to evaluate the vulnerabilities and potential consequences posed by TIH freight rail shipments within each city. To conduct these reviews, TSA uses a systematic and quantitative assessment

methodology, called the Hazard Analysis and Critical Control Point (HACCP), which enables the agency to identify specific locations within a city's rail system that pose a high risk for someone weaponizing a TIH railcar.¹ As part of the assessment, TSA gathers information on the volume and traffic patterns of TIH railcars traveling in and through the city and analyzes these data to identify locations in the city where TIH railcars tend to sit unattended.² These locations are often in freight rail yards or at interchange locations where railroads exchange railcars or break apart and build trains. Once the TSA subject matter experts identify these key locations for each city, they assess them against three risk factors:³

- the potential severity of an attack, such as how many people might be injured or killed by an attack on a TIH car at a location;
- the number of TIH railcars at a specific location; and
- detection capability, such as the ability of police officers or railroad workers to detect an attack before it could be carried out.

Using the HACCP tool and data gathered based on the three risk factors above, TSA calculates a numerical risk score for each location to identify areas on which to focus future security efforts and actions.⁴ However, TSA allows each rail carrier to provide input and clarification on each risk score at a tabletop session the agency holds with the rail carriers at the end of the each review. As of March 2009, TSA completed Corridor Reviews in 12 cities, including the 9 cities originally selected for review in

¹HACCP is a risk management tool used to guide the identification, evaluation, and control of hazards. A hazard is any condition that results in an adverse consequence detrimental to people, property, or the environment. In TSA's case, the hazard is the primary threat scenario.

²For this program, TSA defines unattended railcars as those railcars that are in a train or on railroad-controlled leads or tracks with no crew on board and no personnel active in the area. "Personnel" includes railroad employees or agents, law enforcement officers, private security guards, and rail customer employees.

³According to TSA, these risk factors are comparable to two of the three elements of risk identified in the NIPP. Specifically, TSA's potential severity variable corresponds to consequence, and together, the occurrence and detection variables correspond to vulnerability. TSA officials stated that they considered the threat of an attack to be relatively similar at all locations.

⁴According to a TSA official responsible for the program, initial assessments were less focused on developing and storing data. Thus, TSA lacked summary documentation to ascertain specific information about identified vulnerabilities and consequences or recommendations for improvement. As a result, little information could be gleaned from the earliest assessments in five cities from 2004 to 2006. According to TSA, these limitations were a result of the lack of personnel to conduct these reviews early on.

2004. TSA officials told us that they have assessments under way in 5 cities and plan to continue conducting these reviews in 43 additional U.S. cities that have TIH rail shipments transported through them.

TIH Rail Risk Reduction Program

In 2007, TSA began further assessing the potential vulnerabilities and consequences posed by TIH railcars in major cities by gathering, monitoring, and quantifying risk information associated with TIH rail shipments traveling through 46 U.S. cities.⁵ TSA officials stated that the agency developed this assessment program to measure the progress federal and industry efforts are having in achieving the agency's key performance metric for the freight rail security program, which is to reduce the risk associated with the transportation of TIH in major cities—identified as high-threat urban areas—by 50 percent by the end of 2008. To do so, TSA collected both historical and current information on the number of TIH rail shipments in each city, security at rail yards holding TIH shipments in each city, and city populations. TSA then developed a formula to quantify a risk score for each city. This score is a relative measure, or indicator, of the TIH security risks within a city for a given time period. TSA used the historical information to develop a baseline risk score for each city and then collected later information to measure progress in reducing risk.⁶ Specifically, the agency compiled information for four factors:

- Total hours TIH cars were present inside a city. TSA collected data from the rail industry's automated systems that record the movement and location of all railcars within the U.S. rail system by means of electronic identification tags. TSA used these data to quantify the amount of time TIH railcars are located within a city.
- Security status of TIH cars. TSA collected this information through in-person visits conducted by TSA STSIs at over 200 rail yards located in major cities.
- Population proximity to unsecured TIH cars. TSA used U.S. Census Bureau data to determine the population within a 1-mile radius of each

⁵TSA initially chose these 46 cities to correspond its rail security programs with DHS's Urban Area Security Initiative (UASI) grant program, and refers to these cities as high-threat urban areas. Since TSA's initial list in 2006, the number of high-threat urban areas for the UASI program has increased to 62 cities.

⁶TSA collects rail commodity information on a continual basis, while the agency collects the rest of its information annually, including population proximities and the attended status of TIH railcars.

TIH car that was sitting unattended and to rank each city's possible exposure based on this information.

- City ranking. TSA prioritized the cities' importance on a scale of 1 to 5 (5 being the highest) based on the population of each city.

In 2007, TSA collected historical information on these risks factors from the time period June 1, 2005, to May 31, 2006, to establish a baseline risk score for each of the 46 U.S. cities, and then compared each baseline to information for the current year.^{7,8} Thus far, TSA has determined that nationally there was over a 60 percent reduction in risk from the baseline period to the end of December 2008. However, we have concerns about this performance measure's reported results, as discussed earlier in our report. To show results for this measure, TSA developed a national risk scorecard that ranks each city by risk score. Each Class I rail carrier also receives a unique scorecard, providing insight into its individual TIH risk scores. These scorecards then become the focus of discussions between TSA and individual carriers on how to further reduce risk. TSA officials also said that they may use the scorecards for, among other things, monitoring which cities or railroads have high-risk scores and focusing further assessment and security efforts on these cities or railroads.

Assessments That Included Risks Other Than TIH

TSA Corporate Security Reviews

In 2007, TSA began conducting assessments, called Corporate Security Reviews (CSR), which evaluate potential vulnerabilities associated with a freight rail carrier's corporate security plan and procedures. The purpose of these reviews is to both increase the agency's domain awareness and

⁷Because much of the information TSA uses to assess risk is automated, TSA was able to obtain much of the historical information required for each risk factor. For example, a TSA official responsible for the program told us that TSA determined information on population by obtaining U.S. Census Bureau data. Furthermore, hours of exposure, which is the amount of time the TIH cars are in a city's proximity, was gathered using industry computer commodity tracking data from the freight rail industry.

⁸TSA chose to make its baseline year June 2005 through May 2006 (prior to issuance of the first 24 freight rail security action items). TSA chose to make its baseline year the year before issuance of the action items because it wanted its baseline year to be established prior to implementation of any TSA freight rail security actions.

identify possible vulnerabilities that individual railroad carriers may have because of unique operating procedures or other company-specific concerns. In 2007, TSA conducted CSRs of all seven Class I railroads and assessed their security plans and procedures against the following TSA guidelines: threat assessment and processing; vulnerability assessments; personnel security, auditing/testing of plan; drills/exercises; infrastructure security; hazardous materials security; cybersecurity; and infrastructure security.⁹ The reviews essentially consist of an on-site visit to the carrier's corporate headquarters to interview rail officials on the procedures and processes included in the company's security management plan.¹⁰ After completing its data gathering and analysis, TSA develops a final report for each railroad and sends it to the carrier informing the company of the results. TSA officials told us that overall the Class I carriers have good security plans and procedures in place to respond to raised alert levels. In a few cases, TSA made recommendations for improvement, for example, for better documenting of security processes or protocols and better defining of departmental roles and responsibilities. In 2008, TSA performed CSRs on the three largest short line railroad holding companies that collectively control 89 short line railroads. In the immediate future, TSA intends to focus CSRs on terminal-switching railroads operating within high-threat urban areas. However, TSA has not yet developed a schedule for conducting these reviews.

DHS List of Prioritized Critical Infrastructure

In 2006, DHS IP created a program to annually assess and identify the nation's most critical infrastructure and key resources. This effort results in a prioritized critical infrastructure list. DHS stated that assets on this list—which includes freight rail assets—if destroyed or disrupted could cause national or regional catastrophic effects. This list is used to inform incident management, vulnerability assessments, grants, and other risk management activities. To ensure that assessment resources are invested correctly, DHS IP officials said that DHS works closely with TSA to develop criteria used to determine which freight rail assets should appear

⁹TSA first conducted CSRs in 2004; however, officials said that they do not use the results from these reviews because they changed the criteria used to evaluate the security plans. As such, they decided to reassess the Class I carriers previously evaluated in 2004.

¹⁰During this step, TSA officials may also conduct site visits of various locations, including critical bridges, tunnels, operations centers, and yards.

on the list. They also use information provided from sector industry stakeholders and state homeland security offices.¹¹

DHS IP Infrastructure Vulnerability Assessments

In 2004, DHS IP began two assessment programs to identify vulnerabilities associated with assets and infrastructure in the United States across all sectors of the economy, including freight rail assets. The two programs are BZPP and the SAV program.

BZPP

BZPP is an assessment of an asset's perimeter "outside the fence" to identify potential vulnerabilities associated with these areas where a terrorist may launch an attack.¹² Annually, DHS IP determines which assets and infrastructure are to be subjected to a BZPP assessment by using the DHS prioritized critical infrastructure list. These assets and infrastructure are prioritized by such factors as whether a BZPP assessment was recently conducted and if the asset belongs to a high-risk sector, such as dams or nuclear facilities. DHS IP officials stated that the agency coordinates roughly 200 BZPP assessments a year, and the agency has conducted 53 freight rail-related security assessments since the program's inception. DHS officials called protective security advisors (PSA) are responsible for coordinating BZPP assessments with state and industry stakeholders. These assessments are conducted on a voluntary basis, and the results can be used to obtain grant funding from FEMA for security enhancements.

SAV

These are voluntary visits conducted at the request of an asset owner/operator or the state government. However, PSAs are to solicit state homeland security advisors and major industry officials for SAVs where DHS believes an asset would benefit from the program. DHS officials stated that the agency targets SAVs on (1) a facility or sector that is under threat, (2) a facility that is highly consequential, (3) a facility that supports or is close to a national special security event, (4) a facility that is so complex that it would benefit from subsequent or concurrent BZPP

¹¹DHS determined that the criteria and all numbers related to this list are "For Official Use Only." As a result, these data are not contained in this report.

¹²According to DHS IP officials, there are three main objectives of BZPP: (1) create open communication and coordination among facilities, state and local agencies, and local responders for the protection of the asset; (2) use site-specific buffer zone plans to conduct a gap analysis of state and local capabilities and equipment staffing and training needs; and (3) identify the existing procedures to prevent a terrorist incident to the asset, enhance these procedures, or both.

activities, or (5) a facility whose owner/operator requests an SAV and the facility appears on the DHS prioritized critical infrastructure list. The main distinction between an SAV and a BZPP assessment are that BZPP assessments focus on the outside of the perimeter of an asset and are conducted largely by local law enforcement, while SAVs are conducted by PSAs and focus on vulnerabilities inside the perimeter. The results of the SAV are verbally briefed to the appropriate key staff members of the site upon completion, including any security measures to consider for implementation. However, SAVs are not used to award grants, and the asset owner/operator is not required to adopt any security measures DHS recommends.

Industry Assessments

In 2001, AAR conducted the first nationwide security risk assessment of the freight rail system, which incorporated vulnerability and consequence criteria to evaluate multiple security risks to the freight rail industry.¹³ Overall, the assessment reviewed five critical areas to determine the railroad's security vulnerabilities and consequences: infrastructure, military operations, information technology and communications, train operations, and hazardous materials. For example, the assessment evaluated vulnerabilities and consequences associated with the destruction or degradation of freight rail infrastructure, such as key bridges, tunnels, tracks, and operation centers that electronically direct and monitor train movements.¹⁴ Key participants in the risk assessment included the Class I railroads; ASLRRA; and as appropriate, major chemical industry groups, whose member companies use the rail system to ship TIH commodities.

Individual rail and chemical companies have also conducted assessments of their properties and operations. One impetus for these efforts is the 2003 PHMSA regulations, which require railroads that carry certain hazardous materials—including TIH—and chemical companies that ship these materials to develop security plans that include assessments of the risks of shipments of the covered hazardous materials and measures to mitigate those risks. Officials we interviewed at all 13 of the railroads

¹³AAR, established in 1935, is an organization that represents the Class I freight railroads, some smaller railroads, Amtrak, and some commuter railroads in the United States. AAR also sets the standards for rail operations through the association's committee structure.

¹⁴In a 2008 update to this assessment, the rail industry also identified and prioritized around 1,000 assets, of which about 10 percent were considered highly critical to railroad actions.

**Appendix II: Federal and Industry Freight
Rail Security Vulnerability and Consequence
Assessment Activities Conducted since 2001**

stated that they had conducted these PHMSA-regulated security assessments. In addition to these required assessments, representatives we interviewed from the 7 Class I railroads stated that they conduct other assessments as well, including reviews of TIH operations and physical infrastructure assessments, which have helped them make decisions about business operations and determine where to make physical security upgrades in some cases.

Appendix III: TSA Did Not Consistently Measure Results for Its Key Performance Measure

TSA has made limited progress thus far in measuring the extent to which federal and industry efforts are achieving the agency's only performance metric with a target—to reduce the risk associated with TIH rail shipments in major cities by 50 percent by the end of 2008—because the agency was unable to obtain key data needed to consistently measure results. According to TSA officials, this is the key performance metric for the agency's freight rail security program. Specifically, to measure progress in meeting this metric, TSA has collected limited vulnerability and consequence information from 2007 and compared it with historical vulnerability and consequence information for 2005 and 2006. However, the agency was unable to obtain key information needed to accurately measure vulnerability in 2005 and 2006. As a result, the agency developed a general estimate of this vulnerability using its and industry's expert judgment and inserted it into its calculation of risk for most cities in place of actual historical information that it could not obtain retrospectively. Therefore, the accuracy of this estimated vulnerability—and the associated 60 percent overall reduction in risk that TSA reports as being achieved through November 2008—is uncertain because it depends on the accuracy of the general estimate.¹ More specifically, the key vulnerability risk factor that TSA measures as part of this performance metric is the amount of time that railcars containing TIH are unattended in major U.S. cities. However, TSA was unable to obtain information for this risk factor in 2005 and 2006 because the agency did not begin conducting inspections at rail facilities to gather this information until 2007, yet it was using 2005 and 2006 as its baseline period. Since the 2005 and 2006 vulnerability data were unavailable, agency officials made a broad estimate—hypothesizing that TIH railcars sat unattended during the baseline year, June 2005 through May 2006, approximately 80 percent of the time. TSA officials reported that to develop this estimate, they relied primarily on the memory of railroad employees and their responses to standard questions when they were interviewed by TSA officials during the agency's 2007 inspections at rail facilities. TSA officials also reported that they relied on their expert judgment to develop this estimate. However, because this estimate was based on memories and certain assumptions about past activity rather than actual measurements of unattended cars, which is the type of data that TSA gathered in subsequent years, the improvements that

¹TSA measures risk associated with this metric by gathering and measuring vulnerability and consequence information for various U.S. cities, as discussed earlier in our report. The threat that the agency is measuring vulnerability and consequence against is the threat of someone weaponizing TIH railcars inside the city.

TSA reports have been made in reducing risk depend on the validity of these assumptions and recall.

In addition, we found empirical evidence suggesting that the 2005 and 2006 baseline year data estimate of unattended cars may be inaccurate based on actual data that TSA collected in 2007. Specifically, in reviewing the 2007 data, we learned that the amount of time that TSA inspectors found TIH railcars to be unattended in 2007 varied greatly by city. For example, of the 45 cities that TSA inspected to measure TIH railcar attendance, data for 6 cities inspected in 2007 show cars as unattended 0 percent of the time, and data for 5 other cities show cars as unattended less than 20 percent of the time. Moreover, 18 other cities showed railcars as unattended over 80 percent of the time, including 9 cities showing railcars as unattended 100 percent of the time.² However, the agency was unable to account for any specific actions taken that would explain why the unattended status of TIH railcars seemed to dramatically improve in some cities and slightly worsen in others compared to the agency's estimates. As a result, because TSA cannot resolve the uncertainties associated with its 2005 and 2006 estimate, the accuracy of TSA's risk reduction calculations in subsequent years against the 2005 June through December baseline will likewise remain uncertain. Without being able to show demonstrable reduction in risk related to its only targeted performance measure, TSA does not know the degree to which its programs are effective and does not know which actions are most effective for future rail security efforts. Therefore, we are recommending in this report that TSA take steps to change the baseline measure associated with its TIH risk reduction performance metric to a measure that is more consistent with what has been used in subsequent years, or revise this performance metric to more consistently and accurately assess TIH risk reduction efforts in major cities over time.

²TSA provided TIH railcar unattended status information for 45 cities in 2007. In addition to the cities discussed above, our analysis shows that 4 cities show cars as unattended from 20 to 50 percent of the time, and 7 cities show cars as unattended from 50 to 80 percent of the time. TSA reported that the remaining 5 cities did not have TIH travel in or through them.

Appendix IV: Summary of Key Actions Taken to Secure Freight Rail

The federal government and freight rail industry have taken a range of actions since September 11, 2001, to mitigate freight rail security risks. While many of these actions have focused on securing TIH rail shipments, some actions have addressed other security threats as well. In addition, new TSA and DOT rail security regulations for better securing TIH rail shipments will make some freight rail security actions mandatory. However, federal and industry stakeholders also face some technology challenges to further enhancing the security of TIH rail shipments. These challenges include designing stronger tank cars, developing more real-time railcar tracking and monitoring systems, and substituting highly hazardous materials with less dangerous chemicals. Below is a summary of these various actions, categorized as federal and industry.

Key Federal Actions Taken

TSA Rail Corridor Review Actions

Since 2004, TSA has been assisting freight rail carriers in mitigating security vulnerabilities the agency identified during its Corridor Reviews. Specifically, during these reviews TSA works with individual rail carriers to identify site-specific risk mitigation strategies for areas that pose the greatest risk for weaponizing a loaded TIH railcar. Then, typically at the end of each review, TSA officials propose specific actions that railroads can then either implement at their facilities or as part of their operations to reduce risk. Examples of specific rail carrier actions taken as a result of TSA's reviews follow.

- Following TSA's assessment in New Jersey, rail carriers implemented operational changes that permanently removed railcars containing TIH from three rail yards.
- Also following TSA's assessment in New Jersey, rail carriers installed camera systems to monitor TIH railcars and perimeter fencing. One carrier also installed gates at certain road access points and high-intensity lighting. Some carriers also increased security personnel and the frequency of security patrols at facilities.¹

¹Some physical security enhancements installed at rail facilities in New Jersey were implemented as a result of DHS IP's BZPP assessments.

- Prior to TSA's review in Chicago, two rail carriers would interchange TIH cars at an unmanned location in the city. The lag time between one carrier's drop-off and the other's pickup resulted in loaded TIH cars sitting idle and unattended for significant periods of time in a populated area. As a result of TSA's concern, the two carriers decided to reroute the TIH cars to a different interchange point located outside the city. The rail carriers stated that after they analyzed several options for addressing this vulnerability, they chose to reroute the trains because it adequately addressed TSA's concerns and ended up being more cost effective for them operationally.

TSA and DOT Voluntary Security Action Items

In June 2006, TSA and DOT issued 24 recommended security action items for the rail transportation of TIH materials that addressed system security, access controls, and en route security.² Specific actions included the following:

- designating an individual with overall responsibility for security planning,
- identifying company critical infrastructure,
- collaborating with other railroad security offices,
- restricting access to information the railroad deems to be sensitive, and
- establishing procedures for background checks and safety and security training for contractor employees with unmonitored access to company-designated critical infrastructure.

Then, in November 2006, TSA and DOT issued 3 supplemental security action items for the rail transportation of TIH materials designed to build upon the original 24 and recommended the following:

²System security and access control refer to practices affecting the security of the railroad and its property. En route security refers to the actual movement and handling of railcars containing TIH materials.

- Rail carriers operating in high-threat urban areas should develop site-specific security plans that address the security of the transporting of TIH materials.³
- Rail carriers should not operate trains carrying TIH within a specified distance of public venues with national special security events in progress and as requested by the appropriate agency responsible for overall event security coordination.
- In the security planning process, rail carriers should identify and select areas within their systems where cars containing TIH can be moved and held when threat conditions warrant.

TSA Surface Transportation Inspection Activities

In addition to assisting TSA in measuring industry progress in achieving its 50 percent TIH risk reduction goal, STSIs have also assessed industry's implementation of some of the security action items that TSA and DOT issued in June 2006. Specifically, STSIs visited approximately 151 rail facilities from October through December 2006 and interviewed 2,619 rail employees to assess rail carrier implementation for 7 seven security action items on a scale of high, medium, and low.⁴ When averaged across all carriers, TSA's results showed the level of implementation averaged in the low/medium to medium range. STSIs also conducted an additional set of visits to approximately 147 rail facilities from March through June 2007 to assess the degree to which rail carriers had implemented 10 other security action items.⁵ TSA officials told us that they selected these 10 items for review because they focused more on rail carrier security management

³TSA recommended that each plan (1) reduce the number of hours TIH cars are held in yards, in terminals, and on railroad-controlled leased track in high-threat urban areas; (2) minimize the occurrence of unattended TIH cars in high-threat urban areas; (3) reduce potential exposure to surrounding people, property, and environment in high-threat urban areas with special emphasis on reducing potential exposure to hospitals, high-occupancy buildings, schools, and public venues; (4) reduce the occurrence of standing TIH trains in high-threat urban areas; (5) provide a procedure for the protection or surveillance of unattended TIH trains in high-threat urban areas; (6) ensure compliance with C.F.R. 49 Part 174.14 (48-hour rule); and (7) develop site-specific procedures for the positive and secure handoff of TIH cars at points of origin, destination, and interchange in high-threat urban areas.

⁴Of the rail facilities TSA inspectors visited, about 80 percent were Class I facilities, and of the rail employees the inspectors interviewed, about 75 percent were actual frontline workers. The remaining employees interviewed were considered rail management.

⁵The 10 items TSA selected for review were also part of the original 24 issued in June 2006.

practices than on field-level practices.⁶ TSA's results for these 10 items showed that railroads scored high in the areas of internal communication on threat conditions and establishing liaisons with federal, state, and local law enforcement, but lower in the areas of photo identification, background checks for employees, and intrusion deterrence and detection. While TSA has not conducted any additional surveys of rail carrier implementation of the security action items since 2007, TSA officials stated that item surveys will be an integral part of the 2009 inspection plan. In addition, TSA officials told us that they have conducted approximately 4,000 surveys that provide some information on rail carrier implementation of Supplemental Security Action Item No. 1, which was issued in November 2006; these surveys were components of the TIH Rail Risk Reduction Program and will continue until 2013.

DHS FEMA Grant Funding

Using the states' buffer zone plans and Vulnerability Reduction Purchasing Plan (VRPP) submissions under DHS IP's BZPP, DHS provides grant money, through the states, to local law enforcement agencies that purchase security-related equipment for reducing the risk of the asset assessed to a terrorist attack.⁷ The results of the BZPP assessments are used to develop VRPP, which identifies the spending plan, including the equipment to be purchased under BZPP. VRPP submissions are completed by the local jurisdiction responsible for securing the asset assessed. Once VRPP submissions are completed and submitted to the state administrative agency, DHS verifies that what is planned to be purchased is on the DHS authorized equipment list. As part of the review process, FEMA and DHS IP review the documentation to make sure it is completed appropriately; however, FEMA, as the final approver, ultimately determines whether the funding will be provided and when. Through the end of 2008, DHS told us that it provided \$4.6 million through the program to purchase security-related equipment to protect freight rail assets from terrorist attack. Examples of items purchased include chemical protective

⁶The 10 items TSA selected for review were (1) communication of current threat information; (2) liaison activities with federal, state, and local law enforcement; (3) liaison activities with other railroad security offices; (4) contingency planning; (5) emergency response planning; (6) community safety and security outreach; (7) photo identification and background checks; (8) access control; (9) intrusion deterrence and detection; and (10) secure bridge operation procedures.

⁷Because many rail carriers have their own police forces, BZPP funding was awarded directly to the railroads to purchase security-related equipment.

clothing, bulletproof vests, video surveillance equipment, and portable radios.

National Capital Region Rail Pilot Project

DHS also developed a project to secure rail infrastructure within highly populated or otherwise critical locations. The National Capital Region was chosen for the initial pilot because of the proximity of D.C. rail lines to Congress, the Supreme Court, and other significant entities, monuments, and icons. The National Capital Region Rail Pilot Project (NCRPP) was designed to address security concerns while maintaining efficient rail operations. NCRPP is a remote intelligent video security system-based and sensor-based program that creates a virtual fence of video surveillance cameras along an 8.1 mile rail corridor through Washington, D.C. NCRPP has two central features: a virtual fence surrounding the entire 8.1-mile D.C. corridor and virtual gates installed at each entry point. The virtual fence is made up of a network of video surveillance cameras covering the entire length of the D.C. corridor rail line. The virtual gate design uses nonintrusive remote detection technologies to provide advance notification of approaching train traffic and detect the presence of leaking hazardous and TIH materials. The system architecture allows for easy installation of this system at other critical rail infrastructures throughout the country and provides constant real-time video monitoring and hazardous material detection capabilities. The system also disseminates alarm information to first responders in the NCRPP area, including the U.S. Capitol Police, Washington Metropolitan Police, U.S. Secret Service, White House Situation Room, Federal Bureau of Investigation, and others as determined necessary.

Rail Routing Risk Assessment Tool

In 2005, DHS's Office of State and Local Government Coordination and Preparedness (SLGCP), Office for Domestic Preparedness (ODP), provided a \$5 million grant to the Railroad Research Foundation (RRF) to oversee the development and implementation of three risk assessment tools intended to assist the rail industry and federal government in performing risk assessments, selecting safe and secure rail routes, and implementing a "safe haven" for carriers to use during transport and

storage of TIH railcars so that security risks may be minimized.⁸ However, shortly after RRF began developing the tools, it, in coordination with DHS, elected to condense the three tools into a single Web-based tool that would analyze the safety and security risks along rail routes posed by TIH rail shipments. DHS and RRF officials we spoke with stated that the major factor contributing to this decision was PHMSA's 2006 proposed rail safety and security rulemaking, now a final rule, that requires rail carriers to analyze safety and security risks along the rail routes used to transport certain hazardous materials. RRF, DHS, and other involved stakeholders stated that the tool will provide rail carriers a common framework for conducting this analysis.⁹ RRF and its contractor completed initial development of the tool and held two demonstration briefings on it in November and December 2007. While officials from RRF and DHS and other federal officials we spoke with stated that the briefings effectively demonstrated the tool's ability to host the necessary data, additional funding and work was required to finalize it and make it deployable nationwide. As a result, DHS awarded an additional \$2.5 million grant to RRF in 2008 to finish development of the tool.¹⁰ However, DHS officials

⁸Since 2005, the DHS SLGCP, formerly the DHS Office of Grants and Training (OGT), has moved into FEMA's Grant Program Directorate, Grant Development and Administration Division. The DHS OGT originated within the Department of Justice's Office of Justice Programs in 1998 as the Office for Domestic Preparedness. Pursuant to the Homeland Security Act of 2002, this office was transferred to DHS in March 2003. See Pub. L. No. 107-296, § 403(5), 116 Stat. 2135, 2178 (codified at 6 U.S.C. § 203(5)). In March 2004, the Secretary of Homeland Security consolidated ODP with the Office of State and Local Government Coordination to form SLGCP. SLGCP was created to provide a "one-stop shop" for the numerous federal preparedness initiatives applicable to state and local governments. Recently, SLGCP was incorporated under the Preparedness Directorate as OGT. Pursuant to the Department of Homeland Security Appropriations Act of 2007, OGT was transferred, along with certain other components of the Preparedness Directorate, into FEMA effective March 31, 2007. Pub. L. No. 109-295, § 611(13), 120 Stat. 1355, 1400 (2006).

⁹Other reasons DHS and RRF provided were that TSA and other federal stakeholders that were thought to be possible future users of the tools had indicated that they would not be using the tools because they already had developed their own tools for assessing freight rail risk. In addition, during initial development of the tools, RRF and its contractor determined that the tools were essentially using the same types of data inputs to conduct their analysis and could be easily combined.

¹⁰DHS officials told us that the grant moneys will formally be awarded to CSX Railroad, which has submitted a written letter of intent to DHS stating that it intends to give the entire \$2.5 million award to RRF. DHS said the 9/11 Commission Act required that the department only provide grant funds from the Freight Rail Security Grant Program directly to transportation agencies. As a result, DHS could not provide funding directly to RRF to complete the tool. However, because it was appropriate to have RRF complete the tool, CSX Railroad agreed to accept the grant, as required by law, and provide it to RRF.

also told us that they do not intend to fund any out-year maintenance or updates to the tool, and that it will be up to the rail industry to fund any remaining work.

Although RRF and DHS expect the Rail Routing Risk Assessment Tool to be made available to the railroads in time for them to complete the routing analysis required under PHMSA's final rule, it is uncertain what the impact of this tool will be in making routing decisions because decisions made using the tool can be subjective—depending on the users and how they apply the results of the tool. For example, the contractors assisting RRF in developing the tool said that it is not a “decision-making” tool and it does not make decisions for users on which rail route to use, but rather provides them with a comprehensive set of data on each rail route being analyzed based on the 27 risk criteria outlined in PHMSA's rule. The data are then used to compute a risk score for each route in three categories: security, natural hazards, and accidents. Rail officials can then use the three categorical scores for each route to assist them in determining which routes present the lowest overall risk based on the three scores. However, it is ultimately the user's discretion that determines how the three scores are weighted and interpreted to make a routing decision. As a result, it is uncertain how consistently users of the tool will apply it in their decision making, and rail carriers may view the overall risk posed by commonly used routes differently. The potential differences in decision making—derived from the same tool—could also make it more difficult for FRA to consistently enforce compliance with the rule. Furthermore, the extent to which the tool will be used by the railroads is also uncertain because use of the tool is voluntary, and railroad user groups participating in its development have given mixed feedback on its utility for the analysis.

PHMSA Final Rule

On November 26, 2008, PHMSA issued its final rule requiring rail carriers to compile annual data on certain shipments of explosive, TIH, and radioactive materials; use those data to analyze safety and security risks along rail routes where those materials are transported; assess alternative routing options; and make routing decisions based on those assessments.¹¹ Included in the rule are 27 specific risk criteria rail carriers are required to consider and use when conducting this analysis; however, not all the criteria will be present on each route, and each route will have its own

¹¹Hazardous Materials: Enhancing Rail Transportation Safety and Security for Hazardous Materials Rail Shipments, 73 Fed. Reg. 72,182 (Nov. 26, 2008).

combination of factors to be considered. These criteria cover areas such as rail traffic density of the route, trip length, iconic targets, and population density along the route. Using the results of their analyses, rail carriers must select and use the practicable routes posing the lowest overall safety and security risks.¹² In addition, the rule adopts a new requirement for rail carriers to inspect placarded hazardous materials railcars for signs of tampering or suspicious items, including improvised explosive devices (IED). The rule also clarifies rail carriers' responsibility to address in their security plans' issues related to en route storage and delays in transit. Specifically, the PHMSA rule requires covered entities to include, among other things,

- measures to mitigate risk to population centers associated with in-transit storage;
- procedures for notifying consignees of any significant unplanned delays affecting the delivery of the covered hazardous materials; and
- procedures under which rail carriers will consult with shippers and consignees to minimize the time a railcar containing one of the specified hazardous materials is placed on track awaiting pickup, delivery, or transfer.

FRA plans to review the rail carriers' route analyses on behalf of DOT. FRA intends to have an FRA headquarters team of experts in the various safety disciplines conduct these reviews of the carriers' route analyses; this team is to consult with TSA on security aspects of these analyses. FRA officials indicated that regardless of the risk assessment methodology selected by a rail carrier, FRA is to look at the carrier's analysis for the following information:

- The analysis must demonstrate that the railroad has included the required information, complied with the consultation and other requirements of the

¹²Beginning January 1, 2009, rail carriers must compile information on the commodities they transport and the routes they use for the 6-month period from July 1, 2008, through December 31, 2008. Rail carriers must complete their data collection by March 1, 2009. Rail carriers may either complete the safety and security analyses of routes currently utilized and available alternatives and select the safest, most secure routes for transporting the specified explosive, TIH, and radioactive materials for the period from July 1, 2008, through December 31, 2008, by September 1, 2009, or may notify FRA in writing and complete the process by March 31, 2010, using data for all of 2008. Beginning January 1, 2010, and for subsequent years, rail carriers must compile information on the commodities they transport and the routes used for the previous calendar year and complete route assessments and selections by the end of the calendar year.

PHMSA rule, considered the criteria set out in Appendix D of the rule, and developed a rational explanation for criteria that it is relying on.

- The characterizations of risks and of changes in the nature or magnitude of risks is qualitative and, to the extent possible given available data, quantitative.
- The characterization of risk is broad enough to deduce a range of activities to reduce risks on the lines being analyzed.
- All assumptions, their rationales, and their impact on the risk analysis are clearly set out.
- The analysis considers the full population at risk, as well as subpopulations particularly susceptible to such risks, the populations more highly exposed, or both.
- The analysis adopts consistent approaches to evaluating the risks posed by hazardous agents or events.
- The analysis includes measures to minimize the safety and security vulnerabilities identified through the route analyses.

FRA's enforcement rule sets out the process FRA is to follow if it identifies deficiencies in a railroad's risk analysis; this process includes full consultation with the railroads, PHMSA, TSA, and the Surface Transportation Board before any rerouting would be directed. PHMSA and FRA officials stated that since rail carriers have every incentive to choose routes posing the least overall safety and security risks for moving security-sensitive materials, officials anticipate that FRA will rarely have to overturn a rail carrier's routing decision; more likely, the discussion may center on mitigation measures a carrier can take to reduce the risks that are identified.

PHMSA's Tank Car Safety Proposed Rule

On April 1, 2008, PHMSA and FRA issued a proposed rail safety rule to enhance the performance standards for tank cars used to transport highly hazardous materials, implement operational restrictions to improve accident survivability, and enhance the cars' resistance to rupture or puncture during a derailment.¹³ While this proposed rulemaking focused on safety, DOT officials we spoke with said that these enhancements would also have security benefits. Essentially, the revised standards are designed to improve the accident survivability of railroad tank cars and were developed in response to several rail tank car accidents occurring in recent years in which the tank car was breached and the hazardous product leaked into the atmosphere. Specifically, this rule proposes

¹³73 Fed. Reg. 17,818 (Apr. 1, 2008).

- enhanced tank car performance standards for head and shell impacts, including expedited replacement of tank cars used for the transportation of TIH materials manufactured before 1989 with non-normalized steel head or shell construction;
- operational restrictions for trains hauling tank cars containing TIH materials, such as a maximum speed limit of 50 miles per hour for all railroad tank cars used to transport TIH materials;
- interim operational restrictions for trains hauling tank cars not meeting the enhanced performance standards, for example, a maximum speed limit of 30 miles per hour in nonsignaled (i.e., dark) territory for all railroad tank cars transporting TIH materials or the approval of a complete risk assessment and risk mitigation strategy establishing that operating conditions provide at least an equivalent level of safety as that provided by signaled track; and
- an allowance to increase the gross weight of tank cars that meet the enhanced tank-head and shell puncture-resistance systems.

PHMSA's Tank Car Safety Final Rule

On January 13, 2009, PHMSA and FRA issued a final rule to prescribe enhanced safety measures for the transportation of TIH materials.¹⁴ Pending the issuance of the final rule proposed in April 2008, the rule imposes interim design standards for newly manufactured tank cars. Specifically, this rule requires

- commodity-specific improvements in safety features and design standards, for shell and jacket thickness, for newly manufactured tank cars;
- enhancements in top fittings protection systems and nozzle arrangements for newly manufactured tank cars; and
- a 50 mile per hour speed limit for all loaded rail tank cars used to transport TIH materials.

TSA's Rail Transportation Security Rule

On November 26, 2008, TSA issued a rule establishing security requirements for freight railroad carriers; intercity, commuter, and short-haul passenger train service providers; rail transit systems; and rail operations at certain, fixed-site facilities that ship or receive specified hazardous materials by rail.¹⁵ The rule also codifies the scope of TSA's existing inspection program and requires regulated parties to allow TSA and DHS officials to enter, inspect, and test property, facilities,

¹⁴74 Fed. Reg. 1770 (Jan. 13, 2009).

¹⁵73 Fed. Reg. 72,130 (Nov. 26, 2008).

conveyances, and records relevant to rail security. The rule also requires that regulated parties designate rail security coordinators and report significant security concerns to DHS. This rule further requires that freight rail carriers and certain facilities handling specified hazardous materials be able to report location and shipping information to TSA upon request and to implement chain-of-custody requirements to ensure a positive and secure exchange of specified hazardous materials. TSA also clarifies and amends the sensitive security information (SSI) protections to cover certain information associated with rail transportation.¹⁶ Specifically, TSA's rule requires all rail carriers to

- designate a rail security coordinator and at least one alternate to be available to TSA on a 24-hour, 7-day per week basis to serve as the primary contact for receipt of intelligence information and other security-related activities;
- immediately report incidents, potential threats, and significant security concerns to TSA's Freedom Center; and
- allow TSA officials and other DHS officials to enter and conduct inspections, copy records, perform tests, and conduct other activities necessary to carry out TSA's statutory and regulatory responsibilities.¹⁷

¹⁶Section 114(r) of title 49 of the United States Code requires TSA to promulgate regulations governing the protection of SSI. SSI includes information that would be detrimental to transportation security if publicly disclosed. TSA's SSI regulation, 49 C.F.R. pt. 1520, establishes requirements for the recognition, identification, handling, and dissemination of SSI, including restrictions on disclosure and civil penalties for violations of those restrictions. Although 49 C.F.R. pt. 1520 primarily covers aviation- and maritime security-related information, vulnerability assessments and threat information related to all modes of transportation are considered SSI under 49 C.F.R. §§ 1520.5(b)(5) and 1520.5(b)(7) and must be protected and handled in accordance with 49 C.F.R. pt. 1520. However, because certain other information created in connection with TSA's rule would be detrimental to transportation security if publicly disclosed, TSA's rule amends 49 C.F.R. pt. 1520 to more directly protect information related to the rail sector. Thus TSA's rule adds railroad carriers, rail hazardous materials shippers, rail hazardous materials receivers, and rail transit systems as covered parties under part 1520.

¹⁷This will only be permitted providing that TSA inspectors, and DHS officials working with TSA, will present their credentials for examination at the request of the entity being inspected, with the understanding that the credentials may not be reproduced.

Specific requirements for freight rail carriers and facilities that ship or receive certain hazardous materials include the following:¹⁸

- Freight rail carriers and certain facilities that ship or receive certain hazardous materials by rail must provide to TSA, upon request, the location and shipping information of railcars within their physical custody or control that contain a specified category and quantity of hazardous materials. Class I freight railroad carriers must provide the information to TSA no later than 5 minutes (for one car) or 30 minutes (for two or more cars) after receiving the request. Other railroad operators and rail hazardous materials shipper and receiver facilities must provide the information for one or more cars within 30 minutes after receiving the request.
- As discussed earlier in this report, the rule also requires certain rail carriers, shippers, and receivers to establish and provide for a “secure chain of custody and control” for railcars in their possession containing the selected hazardous materials, such as TIH. Rail carriers, shippers, and receivers are required to establish a secure chain of custody and control through several steps and processes. Specifically, shippers of these hazardous materials are required to perform a physical security inspection of railcars for signs of tampering or suspicious items, including IEDs.¹⁹ During pre-transportation functions, the shipper is also required to store the cars in an area with physical security measures in place until the carrier arrives to pick up the car and assume physical custody of it. The shipper is also required to document the transfer of custody with the rail carrier either in writing or electronically. The rail carrier must also perform an inspection of the cars before leaving the shipper’s facility, as required by DOT. When a carrier transfers a car transporting the hazardous materials to another carrier and the transfer occurs in a high-threat urban area or when the railcar may subsequently enter a high-threat urban area, the transferring carrier must ensure that the railcar is not left unattended at any time during the physical transfer of custody, perform a

¹⁸Transportation of these materials includes (1) a railcar containing more than 2,268 kilograms (5,000 pounds) of a Division 1.1, 1.2, or 1.3 (explosive) material, as defined in 49 C.F.R. § 173.50; (2) a tank car containing a material poisonous by inhalation as defined in 49 C.F.R. § 171.8, including anhydrous ammonia, Division 2.3 gases poisonous by inhalation as set forth in 49 C.F.R. § 173.115 (c), and Division 6.1 liquids meeting the defining criteria in 49 C.F.R. § 173.132(a)(1)(iii) and assigned to hazard zone A or hazard zone B in accordance with 49 C.F.R. § 173.133(a), excluding residue quantities of these materials; and (3) a railcar containing a highway route–controlled quantity of a Class 7 (radioactive) material, as defined in 49 C.F.R. § 173.403.

¹⁹TSA also developed a training video to assist rail carriers in training their employees on how to identify improvised explosive devices and other possible security threats.

security inspection, and document the transfer of custody. When a railroad carrier transfers custody to a rail receiver in a high-threat urban area, the carrier must not leave the car unattended in a nonsecure area until the receiver accepts custody and must document the transfer of custody. In such a transfer, the receiver must ensure that either it or the carrier maintains positive control of the car during the transfer, document the transfer, and keep the car in a secure area until it is unloaded. As used in the regulations, a railcar is “attended” if an employee or authorized representative of the freight railroad carrier (1) is physically located on-site in reasonable proximity to the railcar; (2) is capable of promptly responding to unauthorized access or activity at or near the railcar, including immediately contacting law enforcement or other authorities; and (3) immediately responds to any unauthorized access or activity at or near the railcar either personally or by contacting law enforcement or other authorities. The rule also permits electronic monitoring so long as the responsible party is located on-site and can accomplish an equivalent level of surveillance, response, and notification.²⁰

Key Industry Actions Taken

AAR Industrywide Security Management Plan

AAR’s security plan, developed from the results of the industrywide risk assessment, comprises of four alert levels with specific security actions to be taken by the railroads at each alert level. As the alert level rises, as dictated by the AAR board of directors, the security actions and countermeasures progressively become more rigorous. These actions cover areas such as operations, communications and information technology, hazardous materials shipments, and critical infrastructure. AAR officials said that the primary benefit of the plan is that it allows the industry to tailor and regionalize security measures to the current threat environment, such as a specific geographic area, specific commodities, and so forth. AAR reported that having the ability to tailor security measures to the threat environment is critical because AAR estimates it

²⁰TSA’s rule does not specify any particular category of individual needed to perform this job function and does not specify that a freight carrier would have to use a hazmat employee (as the term is used in 49 C.F.R. § 171.8) to perform this job function. Moreover, to allow freight railroad carriers a maximum degree of flexibility in adopting and implementing procedures to meet the car attendance performance standard, TSA does not specify a maximum number of railcars permitted per attending employee (or authorized representative) or define how close that individual must be to the railcar while attending it.

would cost the rail industry \$500,000 a day to operate nationwide at Alert Level 4. In 2007, AAR began working with its member railroads to update the industrywide plan.²¹ According to AAR, these efforts generally involved restructuring some of the alert level actions and significantly increasing the total number of Alert Level 1 actions. Specifically, AAR reported that because the industry has historically operated at Alert Level 2, many of these actions have become institutionalized by the railroads into their normal day-to-day operations. As a result, the industry feels that moving many of the current Alert Level 2 actions to Alert Level 1 will better reflect the industry's current day-to-day operations. Table 11 contains a brief description of each alert level.

Table 11: AAR Industrywide Security Management Plan's Four Alert Levels

Alert level	Description
Level 1	New normal day-to-day operations: Exists when a general threat of terrorist activity exists, but warrants routine security posture. Actions in effect at this level include conducting security training and awareness activities, restricting certain information to a need-to-know basis, restricting the ability of unauthenticated persons to trace sensitive materials, and periodically testing that security systems are operating as intended.
Level 2	Heightened security awareness: Applies when there is a general nonspecific threat of terrorist activity. Actions in effect at this level include providing security and awareness briefings as part of daily job briefings, conducting content inspections of cars and containers, and increasing security at designated facilities.
Level 3	A credible threat of an attack on the United States or railroad industry (continuously reevaluated): Exists in light of the specificity of the threat against railroad personnel and facilities. Examples of Level 3 actions include further restricting physical access and increasing security vigilance at control centers, communication hubs, and other designated facilities and requesting national guard security for certain critical assets.

²¹AAR reported that many of the updates in its revised plan were identified from prior AAR tabletop exercises conducted in coordination with member railroads. According to AAR, in addition to identifying actions to implement at lower alert levels, the tabletops identified a need to implement and routinely test a better system of implementing the embargo process required at Alert Level 4; enable timely notification to all railroads, customer trade associations, law enforcement agencies, and federal government agencies of an Alert Level 4 embargo action; and monitor passenger carriers' security plans for potential conflicts with freight rail security plans.

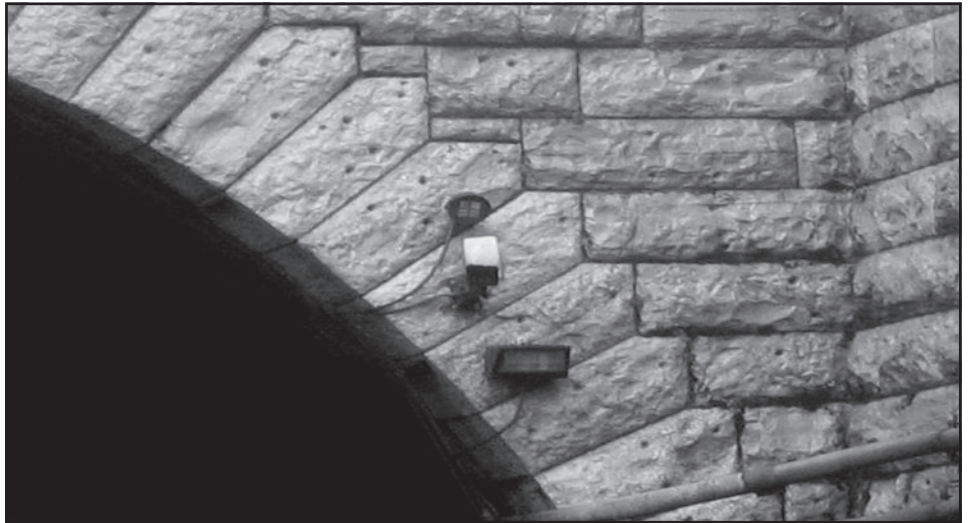
Alert level	Description
Level 4	A confirmed threat of attack against the railroad industry or actual attack in the United States (implemented up to 72 hours and reevaluated): Action taken at this level include stopping the services of non-mission-essential contractors with access to critical facilities and systems, increasing vigilance and scrutiny of railcars and equipment during mechanical inspections to look for unusual items, and providing a continuous guard presence at designated facilities and structures.

Source: GAO.

Actions Taken by Individual Freight Rail Carriers

Rail carriers have also taken a variety of steps to enhance security at some of their facilities by, among other things, installing perimeter fencing, lighting, security cameras, and other monitoring equipment; restricting access through the use of key cards; increasing security awareness; providing security training; and increasing the frequency of security patrols at key yards and facilities. Several rail carriers we visited installed various types of security cameras and monitoring equipment at some of their key rail yards and facilities to better monitor the activities in and around these areas. In addition, some rail carriers had also installed cameras and other surveillance equipment at key bridges. One Class I railroad we met with installed cameras, electronic motion detectors, and sensors to detect a hazardous material release at each end of one of its key tunnels located in a major metropolitan area. Several rail carriers had also installed perimeter fencing and high-intensity lighting around key rail yards and facilities. Figure 4 shows the camera at the tunnel, figure 5 shows lighting that another rail carrier had installed at one of its key rail yards in Houston, and figure 6 shows perimeter fencing at a rail yard in Houston.

Figure 4: Camera System Located in the Upper-Right-Hand Corner of the Tunnel



Source: GAO.

Figure 5: Light Towers at a Rail Yard in Houston



Source: GAO.

Figure 6: Perimeter Fencing at a Rail Yard in Houston



Source: GAO.

Several individual rail carriers we met with also indicated that they implemented other types of measures to better secure their facilities and operations, including creating backup and dual command centers to ensure little or no degradation of service in the event of an attack, requiring employees and contract employees to wear ID badges, installing firewalls and password protecting critical information, increasing the frequency of security patrols at facilities, installing security signage, restricting access to key buildings through the use of key cards, providing security training, and conducting security drills.

Some rail carriers told us that specifically for TIH cars they have increased their temporary storage fees, which are the fees customers pay railroads to temporarily store their railcars at local rail yards if customers cannot

accept the cars when the rail carriers offer them for delivery.²² For instance, one Class I carrier we met with sent a letter to its customers indicating that it was raising its temporary storage fees in 2007 for railcars containing certain hazardous materials, including TIH, to \$500 for the first 24 hours of storage and increasing them to \$1,000 per day for each day of storage thereafter. Another Class I rail carrier we met with is taking steps to require that its TIH customers located in DHS-designated high-threat urban areas accept TIH cars upon arrival. This carrier told us that this change will reduce the time TIH cars sit in its rail yards waiting to be delivered to the customer. However, the carrier also told us that it is providing daily service, including weekends, for some of its TIH customers located in high-threat urban areas to minimize any negative impacts this may have on customer operations. Another rail carrier told us that it is not renewing its fixed-lease track agreements with companies for temporary storage of certain hazardous materials, including TIH.²³ Moreover, several rail carriers we met with said that they are encouraging their rail yard masters to reduce the amount of time TIH cars sit in yards. One carrier stated that its goal is to get all TIH cars processed and out of the high-threat urban areas in less than 24 hours and that any TIH cars that remain in its yards located in a high-threat urban area for more than 24 hours get flagged and get first priority for shipment. Some rail carriers we met with also stated that they have also taken steps to reroute or stop their trains carrying TIH during certain major events. For example, rail carriers we met with indicated that they stopped trains during World Series games, the Final Four basketball tournament, and NFL playoff games.

²²Once a car has been constructively placed at a local serving yard, which is a yard from which the railroad serves local customers, the rail carrier notifies the customer that the car is available for placement at the customer's facility. However, if the customer cannot take the car into its facility upon notification from the railroad, the customer is charged a "demurrage fee" by the railroad. This is a fee the customer pays the railroad for storing the car at the railroad serving yard until the customer can accept the car for final placement at its facility. The amount of money the customer pays in demurrage charges will typically depend on the length of time the car sits in the serving yard before it is accepted for final placement at the customer's facility. Some rail carriers we met with told us that this typically occurs when a customer does not have sufficient space in its facility to accept all the cars it ordered. As a result, it pays the railroad to temporarily store the cars until it has room to receive them in the facility.

²³Leased tracks are railroad tracks in rail yards or railroad sidings that manufacturers, such as chemical companies, lease from a railroad to temporarily store their commodities until needed.

Actions Taken by Individual Chemical Companies

Representatives we interviewed from all six chemical companies stated that they monitor TIH shipments to their destinations using the railroad Automatic Equipment Identification system (AEI) to ensure that cars are continually moving through the rail system.²⁴ Additionally, see the following:

- Two companies said that they are independently installing Global Positioning Systems (GPS) and other detection devices to their tank cars to constantly monitor the shipments and be notified if there is a potential breach in the car.
- Some chemical companies have increased their facilities' security around rail yards, including increasing security guards and installing fencing, cameras, guards, and thermal detection devices around the entire perimeter and points of entry for their railroad infrastructure.²⁵
- One large chemical company we visited in Houston that produces, ships, and receives large amounts of chlorine has completely fenced all of its rail facilities, installed cameras and motion detection sensors at yard entrances, and increased the amount of security lighting and frequency of security patrols. This company also told us that it has seals for its chlorine tank car shipments that require special cutters for removal.²⁶
- During a site visit to a chemical company that routinely receives large quantities of chlorine, we observed several physical security measures that had been installed at the rail receiving facility, such as a crash resistant

²⁴The technology most widely used in the rail industry to track railcar movements is AEI, which is a passive tracking system that tracks each railcar in transit with a unique radio-frequency identification (RFID) tag. The rail industry has placed AEI readers in strategic locations throughout the rail system to detect each RFID tag as it passes the detector. When a railcar, or train, passes a reader, its location is recorded and sent to the railroad; however, the system only indicates that a car is located at a reader, and in some areas AEI readers could be 30 or 40 miles apart. The system provides key information on the trains, including milepost location; locomotives assigned; and consist and car information, such as lading, load status, car specification, origin, and destination.

²⁵Certain chemical facilities are also subject to the DHS Chemical Facility Anti-Terrorism Standards program, which requires facilities that are determined to be high risk to complete site security plans that include measures that satisfy DHS risk-based performance standards.

²⁶The company told us that each seal has a unique serial number, which the company provides to the receiver when shipping either a full or empty car to a customer. The company places two seals on the car, one on the outside and one on the inside for the receiver, when shipping the full or empty car back. As such, both the companies can tell if someone has tampered with a seal. Company officials stated that this is a standard in the chlorine industry.

gate, two barbed wire fences, and several surveillance cameras.²⁷ Figure 7 illustrates some of the fencing installed by this chemical customer.

Figure 7: TIH Rail Customer Facility with Barbed Wire Fencing around the Perimeter



Source: GAO.

²⁷ According to railroad officials we spoke with, they have also worked with this company to establish better procedures for delivery and acceptance of TIH railcars. For example, rail officials told us that when they drop off a shipment of TIH, both railroad and chemical company employees are present, a visual inspection is conducted of the cars, and once that is completed, the gates are opened, the cars are moved inside, and then the gates are closed.

Appendix V: Federal and Industry Stakeholders Also Report Facing Technology Challenges to Enhancing the Security of TIH

Federal and industry stakeholders identified three main technology challenges to better securing TIH shipments, which—if overcome—could improve the security of future TIH shipments. These challenges include designing stronger tank cars, developing more real-time railcar tracking and monitoring systems, and substituting highly hazardous materials with less dangerous chemicals. While federal and industry stakeholders are currently working to meet these challenges, it is too soon to know if these efforts will mitigate the outstanding security risks, as many of these efforts are still under way.

While some federal and industry stakeholder officials we spoke with reported that designing stronger tank cars and better railcar tracking systems and substituting TIH chemicals with less dangerous ones are ways to reduce the security risks these materials pose in transit, they also described technology challenges associated with these efforts. However, stakeholders viewed some of these challenges as more difficult or costly to overcome than others. For example, some stakeholders we spoke with told us that it can be difficult to find substitutes for some chemicals, for example, chlorine, because it is a base product used to make other products. In addition, officials from all six of the chemical companies we met with told us that it can be expensive to switch to alternative chemicals because switching would require them to retrofit facilities to be able to make or use the alternate products and processes. However, while some industry stakeholders identified the challenge of tracking the real-time location or status of railcars while in transit, some stakeholders are finding more real-time ways to track hazardous railcar movements through the use of GPS.

Furthermore, government and industry stakeholders reported that they have been engaged in research aimed at developing safer tank cars that could better withstand an accident or derailment and will be less likely to breach and release dangerous chemicals. However, some rail and chemical industry officials—as well as government officials—reported that it is difficult to develop a tank car that would be resistant to all potential security threats, such as certain types of IEDs, yet would also be safe and have the capacity to carry sufficient amounts of product. Specifically, these stakeholder officials stated that it was difficult to design tank cars such that security improvements to the car—such as reinforcing its hull—do not simultaneously compromise the car’s safety. According to these officials, adding layers to the hull of a tank car increases its weight, which can result in the car being too heavy for the tracks and thus increase the likelihood of its derailment and the resultant potential release of toxic materials. They also reported that they could mitigate the weight concern

by decreasing the capacity of the car, but this would result in more tank cars being put on the rail system to carry the same amount of hazardous materials, thereby increasing the potential risk of an incident as well as congestion in the system. FRA and TSA are also investigating ways to overcome technological challenges, such as researching lightweight coatings that could potentially add ballistics penetration resistance to a tank car without substantially increasing the car's weight. FRA has also tested various products with self-sealant capabilities to protect against a large-caliber weapon creating a gaping hole in a tank car if it was penetrated by a bullet. These officials believe that they may be able to apply these materials to future tank cars, if their weight and costs are not too high, but this research is still under way.

Another technology challenge that stakeholders face relates to developing more sophisticated railcar tracking systems. Currently, the technology most widely used in the rail industry to track railcar movements, AEI, does not provide the real-time location or status of railcars while in transit. Instead, AEI is a passive tracking system that tracks railcars by unique radio-frequency identification tags. When a railcar or train passes a reader, its location is recorded and sent to the railroad. However, the system cannot transmit the precise location of the car, only that it has passed a reader, and in some areas AEI readers could be 30 to 40 miles apart. As a result, some industry stakeholders, including certain chemical companies we contacted, are installing GPS on tank cars as an alternative method of tracking their tank cars from origin to destination.¹ However, these chemical company officials noted that although GPS technology has clear benefits, it can have limitations, such as a limited battery life and problems with signal interference, for example, when a car travels through a tunnel. TSA is conducting a study comparing GPS to the current system, AEI. Results of these studies are expected in 2009.

Lastly, industry stakeholders face technology challenges in attempting to substitute less toxic materials for the highly hazardous materials that currently traverse the freight rail system. While federal and industry officials we interviewed said that substituting highly toxic chemicals with less hazardous materials is one way to reduce risk, chemical industry officials told us that doing so can be expensive, and finding substitutes for

¹A GPS is a satellite-based system that can pinpoint any position on earth—any time and in any weather—and then use receivers to process the satellite signals to determine a location.

some highly hazardous chemicals is especially difficult because these chemicals serve as the bases for other products—and thus do not currently have substitutes. For instance, chlorine is used to develop a wide array of products, including medicines, semiconductors, and paints, in addition to being used for water treatment. Anhydrous ammonia is most commonly used to develop fertilizers to enhance crop growth. While some water treatment facilities have started using chemicals other than chlorine to purify water, some chemical company officials we spoke with said that a substitute for some TIH chemicals has not been identified for all processes. In addition, chemical company officials we spoke with told us that product substitution can be expensive because switching to alternative chemicals would require them to retrofit facilities to be able to make or use the alternate products and processes.

According to some industry stakeholders we spoke with, one alternative to developing substitute chemicals would be to move these materials by pipeline rather than rail or to colocate production and consumption facilities, thereby eliminating the need to transport them by rail. Some chemical industry officials reported that these options could also be potentially costly and would require some retrofitting of chemical facilities. Another alternative shipping option is to move these materials by truck. However, according to officials we spoke with from one large chemical company, the risk of shipping TIH materials by truck is significantly higher than the risk with rail shipments, and as a result, they have elected to not ship by truck. In contrast, some members of the rail industry we spoke with supported these alternatives, recognizing that these measures would reduce the volume of highly hazardous materials on the rail system and concurrently reduce their security risks and liability concerns.

Appendix VI: Summary of 9/11 Commission Act Requirements Pertaining to Freight Rail Security

The 9/11 Commission Act, signed into law on August 3, 2007, requires federal stakeholders to take several additional steps to further secure the freight rail system, including TIH shipments. Table 12 provides a listing of the key provisions in the act that are relevant to freight rail security.

Table 12: Key Provisions from the 9/11 Commission Act That Are Relevant to Freight Rail Security

Provision	Description
Sec. 1202: Transportation Security Strategic Planning	<ul style="list-style-type: none"> • Specifies that the transportation modal security plan required under 49 U.S.C. § 114(t) must include threats, vulnerabilities, and consequences. • Requires that the National Strategy for Transportation Security (NSTS) include a 3-year and a 10-year budget for federal transportation security programs that will achieve the priorities of the NSTS, methods for linking the individual transportation modal security plans and a plan for addressing intermodal transportation, and transportation modal security plans. • Requires the Secretary of Homeland Security, in addition to submitting an assessment of the progress made on implementing the NSTS, to submit an assessment of the progress made on implementing the transportation modal security plans. • Requires that the progress reports include an accounting of all grants for transportation security; funds requested in the President’s budget for transportation security, by mode; personnel working on transportation security, by mode; and information on the turnover in the previous year among senior staff working on transportation security issues. • Requires that the NSTS include the TSSP required by Homeland Security Presidential Directive 7.
Sec.1304: Surface Transportation Security Inspectors	<ul style="list-style-type: none"> • Authorizes the Secretary to train, employ, and utilize STSIs. • Requires the Secretary to employ up to a total of <ul style="list-style-type: none"> • 100 STSIs in fiscal year 2007, • 150 STSIs in fiscal year 2008, • 175 STSIs in fiscal year 2009, and • 200 STSIs in fiscal years 2010 and 2011. • Requires the DHS Inspector General, not later than September 30, 2008, to submit a report to the appropriate committees on the performance and effectiveness of STSIs, whether there is a need for additional inspectors, and other recommendations.
Sec. 1511: Railroad Transportation Security Risk Assessment and National Strategy	<ul style="list-style-type: none"> • Requires the Secretary to establish a federal task force to complete, within 6 months after enactment (Feb. 3, 2008), a nationwide risk assessment of a terrorist attack on railroad carriers. • Requires the Secretary to develop and implement, not later than 9 months after enactment (May 3, 2008), the modal plan for railroad transportation, as required by 49 U.S.C. § 114(t). • Requires the Secretary to transmit to the appropriate congressional committees, not later than 1 year after enactment (Aug. 3, 2008), the assessment and national railroad strategy and an estimate of the cost to implement the strategy. • Consistent with the requirements of 49 U.S.C. § 114(t), requires the Secretary to update the assessment and strategy each year and submit a report containing the assessment and report.

**Appendix VI: Summary of 9/11 Commission
Act Requirements Pertaining to Freight Rail
Security**

Provision	Description
Sec. 1512: Railroad Carrier Assessments and Plans	<ul style="list-style-type: none"> • Requires that \$5 million out of the funds authorized by this act be made available to the Secretary for fiscal year 2008 to carry out this section. • Requires the Secretary to assign each railroad carrier to a risk-based tier. • Authorizes the Secretary to establish a security program for railroad carriers not assigned to the high-risk tier. • Requires the Secretary, not later than 12 months after enactment (Aug. 3, 2008), to establish standards and guidelines for developing and implementing the vulnerability assessments and security plans for railroad carriers assigned to high-risk tiers. • Requires the Secretary, not later than 12 months after enactment (Aug. 3, 2008), to issue regulations that require each railroad carrier assigned to a high-risk tier to conduct a vulnerability assessment and prepare, submit to the Secretary for approval, and implement a security plan. • Requires railroad carriers assigned to a high-risk tier to submit vulnerability assessments and security plans to the Secretary for approval not later than 9 months after the date of issuance of the regulations. • Requires the Secretary to provide technical assistance and guidance to railroad carriers in conducting vulnerability assessments and to require that each vulnerability assessment include certain factors. • Requires the Secretary to provide technical assistance and guidance to railroad carriers in preparing and implementing security plans and to require that each security plan include certain factors. • Requires the Secretary to provide threat information that is relevant to the carrier to appropriate employees of a railroad carrier. • Requires the Secretary, within 6 months of receiving the assessments and security plans, to review each assessment and security plan, require amendments to any security plan that does not meet the applicable requirements, and approve any vulnerability assessment or security plan that meets the applicable requirements. • Authorizes the Secretary to require railroad carriers, during the period before the deadline for submitting the assessments and security plans, to submit a security plan to implement any necessary interim security measures essential to providing adequate security. • Authorizes the Secretary to determine that existing procedures, protocols, and standards meet all or part of the requirements of this section and authorizes the railroad carriers to comply with existing procedures, protocols, and standards that meet the requirements of this section. • Requires each railroad carrier that submitted a vulnerability assessment and security plan and is still assigned to the high-risk tier to submit to the Secretary an evaluation of the adequacy of the vulnerability assessment and security plan not later than 3 years after the vulnerability assessment and security plan are approved by the Secretary, and at least once every 5 years thereafter, and requires the Secretary to review the evaluation within 180 days of submission.
Sec. 1513: Railroad Security Assistance	<ul style="list-style-type: none"> • Authorizes the Secretary to make grants to railroad carriers, the Alaska Railroad, security-sensitive materials shippers that ship by railroad, owners of railroad cars used in the transportation of security-sensitive materials, state and local governments for railroad passenger facilities and infrastructure not owned by Amtrak, and Amtrak for specified intercity passenger railroad and freight railroad security improvements. • Establishes that any railroad carrier that has an approved vulnerability assessment and security plan and any carrier that uses the grant funds solely to develop an assessment or security plan is eligible for grant funds, and authorizes the Secretary, prior to the earlier of 1 year after the date of issuance of final regulations requiring

**Appendix VI: Summary of 9/11 Commission
Act Requirements Pertaining to Freight Rail
Security**

Provision	Description
	<p>vulnerability assessments and security plans or 3 years after the date of enactment (Aug. 3, 2010), to award grants to carriers based on vulnerability assessments and security plans that the Secretary deems are sufficient for the purposes of this section but that have not been approved by the Secretary.</p> <ul style="list-style-type: none"> Requires the Secretary to determine the requirements for recipients of grants, establish priorities for uses of funds for grant recipients, award the funds based on risk, take into account whether stations or facilities are used by commuter railroad passengers as well as intercity railroad passengers, encourage nonfederal financial participation in projects funded by grants, and not later than 5 business days after awarding a grant to Amtrak, transfer grant funds to the Secretary of Transportation to be disbursed to Amtrak.
Sec. 1516: Railroad Carrier Exercises	<ul style="list-style-type: none"> Requires the Secretary to establish a program for conducting security exercises for railroad carriers.
Sec. 1517: Railroad Carrier Training Program	<ul style="list-style-type: none"> Requires the Secretary, not later than 6 months after enactment (Feb. 3, 2008), to develop and issue regulations for a training program to prepare railroad frontline employees for potential security threats and conditions. Requires each railroad carrier, not later than 90 days after the Secretary issues the regulations, to develop a security training program in accordance with the regulations and submit the program to the Secretary for approval. Requires the Secretary, not later than 60 days after receiving a security training program, to approve the program or require the operator to make revisions. Requires the carrier to respond to the Secretary's comments not later than 30 days after receiving them. Requires the carrier, not later than 1 year after the Secretary approves a security training program, to complete the training of all railroad frontline employees who were hired more than 30 days preceding such date, and requires the carrier to complete training for employees employed less than 30 days preceding such date within their first 60 days of employment. Requires the Secretary to periodically review and update, as appropriate, the training regulations to reflect new or changing security threats. Requires the Secretary, not later than 2 years after the issuance of the regulations, to review implementation of the training program of a representative sample of railroad carriers and frontline employees and submit a report to the appropriate committees.
Sec. 1518: Railroad Security Research and Development	<ul style="list-style-type: none"> Requires the Secretary, acting through the Under Secretary for Science and Technology and the Administrator of TSA, to carry out a research and development program to improve the security of railroad transportation systems.
Sec. 1519: Railroad Tank Car Security Testing	<ul style="list-style-type: none"> Requires the Secretary to conduct a vulnerability assessment of railroad tank cars used to transport TIH materials. Requires the Secretary, acting through the National Infrastructure Simulation and Analysis Center, to conduct an air dispersion modeling analysis of release scenarios of TIH materials resulting from a terrorist attack on a loaded railroad tank car.
Sec. 1520: Railroad Employee Security Threat Assessments	<ul style="list-style-type: none"> Requires the Secretary, not later than 1 year after enactment (Aug. 3, 2008), to complete a name-based security background check against the consolidated terrorist watchlist and an immigration status check for all railroad frontline employees.
Sec. 1522: Procedural Requirements for Railroad Employee Security Threat Assessments	<ul style="list-style-type: none"> Requires the Secretary, if the Secretary issues any guidance, recommendations, suggested action items, or any other widely disseminated voluntary action items related to security background checks of railroad employees, to include recommendations on the appropriate scope and application of a security background check and a redress process for adversely affected individuals.

**Appendix VI: Summary of 9/11 Commission
Act Requirements Pertaining to Freight Rail
Security**

Provision	Description
	<ul style="list-style-type: none"> • Requires the Secretary, if the Secretary issues any rule, regulation, or directive requiring a railroad carrier to perform a security background check of employees, to prohibit the carrier from making an adverse employment decision unless the carrier determines that the employee has been convicted, has been found not guilty by reason of insanity, or is under want, warrant, or indictment for a permanent disqualifying criminal offense, as defined for the Transportation Worker Identification Credential (TWIC) program in 49 C.F.R. pt. 1572; was convicted or found not guilty by reason of insanity of an interim disqualifying offense, as defined for the TWIC program in 49 C.F.R. pt. 1572, within 7 years of the date of the background check; or was incarcerated for an interim disqualifying offense and released from incarceration within 5 years of the date of the background check. • Requires the Secretary, if the Secretary issues any rule, regulation, or directive requiring a railroad carrier to perform a security background check of employees, to provide an adequate redress process for an employee subjected to an adverse employment decision that is consistent with the appeals and waiver process established for the TWIC program in 46 U.S.C. § 70105(c), and to have the authority to order an appropriate remedy if the Secretary determines that a carrier wrongfully made an adverse employment decision. • Prohibits a carrier from knowingly misrepresenting to an employee or other relevant person the scope, application, or meaning of any rules, regulations, directives, or guidance issued by the Secretary related to security background checks.
<p>Sec. 1524: International Railroad Security Program</p>	<ul style="list-style-type: none"> • Requires the Secretary to develop a system to detect both undeclared passengers and contraband, with a primary focus on the detection of nuclear and radiological materials entering the United States by railroad. • Requires the Secretary to identify and seek the submission of additional data elements for improving high-risk targeting of cargo prior to importation into the United States, utilize data collected and maintained by the Secretary of Transportation in the targeting of high-risk cargo, and analyze the data to identify high-risk cargo for inspection. • Requires the Secretary to transmit to the appropriate committees a report that describes the progress of the system being developed.
<p>Sec. 1551: Railroad Routing of Security-Sensitive Materials</p>	<ul style="list-style-type: none"> • Requires the Secretary of Transportation, not later than 9 months after enactment (May 3, 2008), to publish a final rule based on PHMSA's Notice of Proposed Rulemaking published on December 21, 2006. • Requires the Secretary of Transportation to ensure that the final rule requires each railroad carrier transporting security-sensitive materials in commerce, not later than 90 days after the end of each calendar year, to compile security-sensitive materials commodity data. • Requires the Secretary of Transportation to ensure that the final rule requires each railroad carrier transporting security-sensitive materials in commerce to provide, for each calendar year, a written analysis of the safety and security risks for the transportation routes identified in the security-sensitive materials commodity data. • Requires the Secretary of Transportation to ensure that the final rule requires each railroad carrier transporting security-sensitive materials in commerce, for each calendar year, to identify practicable alternative routes over which the railroad carrier has authority to operate and perform a safety and security risk assessment of each alternative route. • Requires the Secretary of Transportation to ensure that the final rule requires each railroad carrier transporting security-sensitive materials in commerce to use the required analysis to select the safest and most secure route to be used in transporting security-sensitive materials.

**Appendix VI: Summary of 9/11 Commission
Act Requirements Pertaining to Freight Rail
Security**

Provision	Description
	<ul style="list-style-type: none"> Requires the Secretary of Transportation to ensure that the final rule requires each railroad carrier transporting security-sensitive materials in commerce, not less than once every 3 years, to analyze the route selection determinations required under this section to review all operational changes, infrastructure modifications, traffic adjustments, changes in the nature of high-consequence targets located along or in proximity to the route, or other changes affecting the safety and security of the movements of security-sensitive materials that were implemented since the previous analysis was completed.
Sec. 1552: Railroad Security-Sensitive Material Tracking	<ul style="list-style-type: none"> Requires the Secretary to develop a program that will encourage the equipping of railroad cars transporting security-sensitive materials with technology that provides car position location and tracking capabilities and notification of railroad car depressurization, breach, unsafe temperature, or release of hazardous materials, as appropriate.
Sec. 1555: Hazardous Materials Security Inspections and Study	<ul style="list-style-type: none"> Requires the Secretary of Transportation to consult with the Secretary of Homeland Security to limit, to the extent practicable, duplicative reviews of hazardous materials security plans. Requires the Secretary of Transportation, in conjunction with the Secretary of Homeland Security, within 1 year after enactment (Aug. 3, 2008), to study the extent to which insurance, security, and safety costs borne by railroad carriers, motor carriers, pipeline carriers, air carriers, and maritime carriers associated with the transportation of hazardous materials are reflected in the rates paid by offerors of such commodities as compared to the costs and rates for the transportation of nonhazardous materials.

Source: GAO analysis of Pub. L. No. 110-53, 121 Stat. 266. (2007).

Appendix VII: Comments from the Department of Homeland Security

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



**Homeland
Security**

April 7, 2009

Ms. Cathleen A. Berrick
Director, Homeland Security and Justice Issues
U.S. Government Accountability Office (GAO)
441 G Street, NW
Washington, DC 20548

Dear Ms. Berrick:

The Department of Homeland Security (DHS) would like to thank you for the opportunity to comment on the GAO-09-243SU draft report titled, "*Actions Have Been Taken to Enhance Security, but the Federal Strategy Can Be Strengthened and Security Efforts Better Monitored*". The Transportation Security Administration (TSA) values the investigative team's comprehensive review of this Agency's progress in addressing freight rail security needs and intends to immediately implement its recommendations. TSA also wishes to express our appreciation for the professionalism demonstrated by GAO's team members in conducting this difficult and broad-ranging review.

This letter responds to the recommendations made by the GAO and provides current information on the status of programs referred to in the draft report. The following activities have occurred within TSA since our last conversation with the GAO review team on December 10, 2008.

Corridor Assessments

In early 2004, the Homeland Security Council (HSC) requested that DHS and the U.S. Department of Transportation (DOT) conduct risk assessments specifically examining the movement of tank cars used for the bulk shipment of toxic inhalation hazard (TIH) materials in nine urban areas: Washington, DC, Northern New Jersey, Cleveland, New Orleans, Buffalo, Houston, Chicago, Philadelphia, and Los Angeles. These nine areas were part of a larger list of 46 High Threat Urban Areas (HTUAs) defined by DHS. These risk assessments are known as Freight Rail Comprehensive Reviews or Freight Rail Corridor Assessments (Comprehensive Review). TSA has conducted seven Comprehensive Reviews involving over a dozen railroad companies.

A Comprehensive Review is comprised of three distinct phases. The first is the fact gathering phase. During this phase, TSA determines the distinct geographic area that comprises the Corridor under assessment. Once the Corridor area has been determined, the TSA team conducts research to determine the locations of shippers, receivers, and rail

- 2 -

facilities that handle tank cars with TIH materials. A request for information is sent to the railroads operating within the Corridor to provide TSA staff with an overview of railroad operations in the area. Potential locations of interest, known as security control points (SCPs), are identified for inclusion in on-site evaluations that are conducted in phase two.

The second phase is the analysis phase. During this phase, TSA, along with representatives of the participating railroads and other Government partners, conducts on-site security evaluations of locations identified in the fact gathering phase. Analysis of the information gathered during the on-site evaluations is used to identify gaps in preparedness and countermeasures. Locations initially identified as areas of concern may be removed as a result of information gathered during the on-site visits. Preliminary options for consideration are identified and noted during this phase.

The third phase is the options for consideration phase. During this phase, a tabletop exercise is conducted with representatives from TSA, participating railroads, and other Government partners to review all SCPs visited during phase two. Options for consideration that are developed at the tabletop exercise are presented in a report and include countermeasures, security enhancements, and mitigation strategies based on team member observations and analysis of factual information. The railroads use this experience and information to develop and implement methods to continue this cooperative process in reducing vulnerabilities associated with TIH shipments moving through HTUAs.

In addition to completing the risk assessments directed by the HSC in the nine metropolitan areas listed above, TSA has also completed assessments in Sacramento, Oklahoma City, and Baltimore. Additional assessments are currently underway in Denver, Milwaukee, Charlotte, Little Rock, and Atlanta.

Between 2006 and 2008, the DHS Urban Area Security Initiative (UASI) list¹ has grown from 46 to 60 locations. TSA has leveraged the resources of the Surface Transportation Security Inspectors (STSI) and plans to conduct assessments in the remainder of the 60 HTUAs as itemized in the 2009 DHS UASI list.²

STSI Program

The STSI program deploys 175 inspectors in 54 field offices to conduct surveys and inspections of freight rail and other surface transportation operations throughout the Nation. The efforts of the inspectors are focused on the HTUAs of highest risk in the freight rail industry. The inspection program is responsible for verifying implementation of voluntary security measures, conducting vulnerability assessments, and conducting regulatory compliance inspections. In addition to participating in Corridor Assessments, which feed recommendations to TSA leadership, the inspectors also act as local liaisons to railroad carriers and other Government agencies for emergency planning and response. This

¹ The UASI list includes areas eligible for DHS homeland security grants.

² TSA has trained three STSI teams on Corridor Assessment methodology. TSA's Office of Transportation Sector Network Management plans to coordinate with the Office of Security Operations to train additional teams and will optimize the use of those teams during the conduct of the future assessments planned for the remainder of the 60 HTUAs.

- 3 -

important component of layered security will expand in fiscal year (FY) 2009 to 225 inspectors nationwide.

Corporate Security Reviews (CSR)

CSRs evaluate and collect physical and operational preparedness information including critical asset and key point-of-contact lists; review emergency procedures and domain awareness training; and provide an opportunity to share industry best practices. Since the inception of the TSA Freight Rail Division in 2002, TSA has worked closely with railroad carriers to determine the level of security throughout the industry and to improve it. In coordination with freight rail stakeholders, TSA has issued guidelines and recommended protective measures to enhance freight rail security, particularly as it applies to the risk associated with the transportation by rail of TIH materials. Among other things, TSA's guidelines recommended that railroad carriers develop and implement security plans. Measures railroad carriers have taken through this voluntary program have resulted in an overall risk reduction of more than 60 percent, well above the target reduction of 50 percent. The CSR program not only assesses how a freight railroad carrier's security plan addresses the transportation of hazardous materials, but also reviews and assesses the effectiveness of those plans in the following areas:

- Communication of Security Plan
- Audit of Security Plan
- Cyber Security
- Protection of Critical Assets
- Security Awareness Training
- Personnel Security
- Threat Assessment

In addition, the CSRs also provide carriers an opportunity to update TSA on system-wide improvements as they relate to the implementation of the security plan.

In 2008, TSA updated the methodology and format of the CSRs to facilitate comparative scoring metrics that will enable TSA and industry stakeholders to identify best practices. In addition, TSA has conducted CSRs on railroad entities that exercise operating control over 98 short line, regional, and terminal railroads. During FY 2009, TSA plans to revisit Class I railroads utilizing the new methodology to assess the improvements and security enhancements that have taken place since the original CSRs were conducted in FY 2007.

TSA Rail Security Rule

On November 26, 2008, TSA issued a final rule on rail transportation security aimed at strengthening the security of the Nation's freight and passenger rail systems, including reducing the risk associated with the transportation of security-sensitive materials, including TIH materials, 73 FR 72130. While TIH materials represent less than one percent of all hazardous materials rail shipments, these materials are potentially lethal and include essential chemicals such as chlorine and anhydrous ammonia. The final rule requires that freight railroad carriers, rail hazardous materials shippers, rail hazardous materials receivers, and passenger rail carriers (including passenger railroad carriers and rail transit systems) allow TSA and DHS officials to enter, inspect, and test property, facilities, conveyances, and

- 4 -

records relevant to rail security. The regulated parties must also designate rail security coordinators and report significant security concerns to TSA.

In the case of freight rail, the final rule requires freight railroad carriers and certain facilities handling specified hazardous materials to be able to report location and shipping information to TSA upon request, and implement chain of custody requirements to ensure a positive and secure exchange of rail security-sensitive materials.

Information Sharing

In response to the statements on pages 64-65 of the report concerning information sharing by the Association of American Railroads (AAR) with the DHS Office of Infrastructure Protection (IP), we are confident that the Protected Critical Infrastructure Information (PCII) Program and the protections embodied in the Sensitive Security Information (SSI) law and regulations can meet the needs of AAR to protect the critical infrastructure information it shares with DHS. The PCII Program is a voluntary program that the private sector may use to protect its most sensitive information when shared with the Government. IP is currently in discussions with AAR on sharing their critical infrastructure list through PCII, but ultimately it is the association's decision whether the information will be submitted to DHS. Sensitive Security Information (SSI) is a specific category of information related to transportation security that requires protection against public disclosure. Although it is not classified national security information, SSI is a category of sensitive but unclassified information that, along with PCII, is specifically exempted by statute from release under the Freedom of Information Act (FOIA), and is to be disclosed only to covered persons on a need to know basis. While SSI may be shared with regulated entities, the public disclosure of information obtained or developed in the conduct of security activities is generally prohibited.

Infrastructure Assessment

The TSA Freight Rail Division is developing an initiative to address the security of critical railroad infrastructure. As of March 2009, we have created a draft risk tool to identify critical freight rail infrastructure and measure the relative risk associated with it. The tool will first focus on railroad bridges, and then another version will be developed to measure relative risk to tunnels and other railroad infrastructure. The tool will be similar in design to HACCP (Hazard Analysis and Critical Control Point) which was developed to measure the relative risk of bulk TIH in densely populated areas. The TSA infrastructure tool will measure criticality and vulnerability.

We have scheduled meetings with several Class I freight railroad carriers to seek their input and comment on the infrastructure tool. The first meeting of this type took place March 10, 2009. We plan to roll out our assessment tool at an Intermodal Security Training and Exercise Program (ISTEP) workshop with industry security partners in summer 2009. When the tool is finalized, we will begin assessing the railroad crossings over the Mississippi, Ohio, and Missouri rivers. Additionally, TSA STSIs will use the tool to assess critical railroad infrastructure in HTUAs in which they conduct Corridor Reviews.

- 5 -

DHS Freight Rail Security Grant Program (FRSGP)

The FRSGP was created as a new component of the Transit Security Grant Program (TSGP) in FY 2008. The TSGP is one of five DHS programs that focus on infrastructure protection activities with a primary focus on strengthening the Nation's critical infrastructure against terrorism. In FY 2008, the FRSGP provided \$7.4M to railroad operators that transport security-sensitive materials through HTUAs. Class I freight railroad carriers whose annual operating revenues exceed \$319.2 million may request funds to support security awareness and emergency response training for frontline employees provided they have completed an acceptable vulnerability assessment and security plan. Class II freight railroad carriers whose annual operating revenues are between \$25.5M and \$319.2M, and Class III freight railroad carriers whose annual operating revenues are less than \$25.5M may request funds to conduct a vulnerability assessment and develop a security plan. The Class II and Class III freight railroad carriers may also request funds to support security awareness and emergency response training for frontline employees if they have completed an acceptable vulnerability assessment and security plan.

The FY 2009 FRSGP applications are expected to be awarded the spring of 2009. This year's \$15M grant program builds on the FY 2008 programs regarding Security Plan, Vulnerability Assessments, and Frontline Railroad Employee Training. In addition to these important programs, TSA included a new program to encourage the railroad industry to start utilizing GPS-based tracking solutions to monitor their high risk assets as they move through HTUAs. The GPS program will provide the tank car owners and operators the resources to install GPS tracking devices on bulk-TIH tank car shipments, which will enhance the protection and visibility of these dangerous commodities.

The following represents the Department of Homeland Security's response to the recommendations made by the GAO:

Recommendation 1: To ensure that the Federal strategy to secure the freight rail system is comprehensive and considers a wider range of risk information, develop a plan for addressing identified security threats to freight rail other than toxic inhalation hazard (TIH), such as the destruction of or sabotage to freight rail bridges and tunnels and cyber attacks to the rail system, and incorporate this information and other related strategic updates into its Freight Rail Modal Annex. As part of this effort, further evaluate methods for estimating the likelihood of various threats occurring and ensure that this information is also considered when developing future risk assessments and strategic updates.

TSA Concurs: In accordance with Section 1511 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*, TSA is collecting comments from railroad management, labor organizations representing railroad employees, owners or lessors of railroad cars used in the transport of hazardous material, emergency responders, offerors of security-sensitive materials and public safety officials regarding the National Strategy for Railroad Security. This stakeholder input was considered during the development of the national strategy and will provide additional guidance during its implementation. In addition, the TSA Freight Rail Division is developing an initiative to address the security of critical railroad infrastructure. TSA has created a draft risk tool designed to identify critical freight rail infrastructure and measure the relative risk associated with it. The tool will measure criticality and vulnerability

- 6 -

and will initially focus on railroad bridges. Ensuing versions of the tool will be developed by TSA to measure relative risk to tunnels and other infrastructure. TSA has scheduled meetings with several Class I freight railroad carriers to seek their input and comment on the infrastructure tool. The first meeting of this type occurred on March 10, 2009. We plan to roll out our assessment tool at an ISTEP (Intermodal Security Training and Exercise Program) workshop with industry security partners in summer 2009. When the tool is finalized, we will begin assessing the railroad crossings over the Mississippi, Ohio, and Missouri rivers. Additionally, TSA Surface Transportation Security Inspectors (STSI) will use the tool to assess critical railroad infrastructure in High Threat Urban Areas as they conduct Corridor Reviews.

Recommendation 2: To better ensure that relevant Federal and industry partners effectively leverage their resources to achieve the strategic vision of TSA's Freight Rail Modal Annex, TSA should ensure that future updates to its Annex more comprehensively address factors contained in Executive Order 13416 and identified key characteristics of a successful national strategy including:

- describing the methodology used to develop the strategy and which organizations and entities contributed to its development;
- more clearly defining Federal and industry roles and responsibilities;
- ensuring that performance measures have defined targets and are linked to fulfilling goals and objectives;
- more systematically addressing specific milestones for completing activities and measure progress toward meeting identified goals;
- more thoroughly identifying the resources and investments required to implement the strategy, including priorities for allocating future grants; and
- more comprehensively identifying linkages with other developed strategies such as those that guide DHS IP, whose responsibilities overlap with TSA for protecting freight rail critical infrastructure.

TSA Concur: TSA endorses the elements detailed in recommendation 2. TSA incorporates many of those elements into the Freight Rail Modal Annex. Future updates of TSA's Freight Rail Modal Annex will be designed to more specifically address issues such as stakeholder roles and linkages, goal oriented milestones, performance measures, and future resource requirements.

Recommendation 3: To ensure that TSA is consistently and accurately measuring agency and industry performance in reducing the risk associated with TIH rail shipments in major cities, take steps to revise the baseline year associated with its TIH risk reduction performance measure to enable the agency to more accurately report results for this measure.

TSA Concur: TSA recognizes the importance of establishing outcome-based performance measures for any and all programs developed and implemented to strengthen security. TSA will establish a new 12-month baseline in which the data is empirical and qualified by TIH Risk Reduction Surveys. Current year performance will be compared to the new baseline period and scored to determine variance. In addition, in an effort to maintain consistency, provide historical perspective, and to discern the effectiveness of the voluntary Security Action Items (SAI), TSA will continue to measure and score current performance and

- 7 -

compare it to the original baseline that is comprised of the 12-month period preceding the adoption of the SAIs, but in doing so, will provide sufficient information with regard to possible data limitations.

Recommendation 4: To ensure that TSA is able to more effectively assess the progress being made in securing freight rail, balance future activities against the various security risks to freight rail, and use its and industry's resources in the most cost effective manner, take steps to more fully track and assess the implementation and effectiveness of security actions being taken to secure freight rail.

TSA Concurs: TSA will continue to track the level of industry SAI adoption and implementation as well as compliance with 49 CFR part 1580 through STSI inspections of railroad carrier locations and operations. The additional perspective gained by measuring TIH risk reduction performance against the previous year will enable TSA to determine the efficacy of freight rail initiatives and security actions as they are being implemented. TSA will continue to track TIH dwell time and assess the level of attendance for loaded TIH rail cars by High Threat Urban Area and by freight railroad carrier. In addition, Corporate Security Reviews will provide insights into system-wide improvements effected by freight railroad carriers as they occur and, when compared to the current assessments, shed light on the effectiveness of those improvements.

Recommendation 5: To better ensure that Federal agencies are coordinating as effectively as possible, work with Federal partners, such as DHS-IP and the Federal Railroad Administration (FRA), to ensure that all relevant assessments and information are shared and TSA and FRA field inspector resources are fully leveraged.

TSA Concurs: Recognizing the importance of having and maintaining strong working relationships with other Government agencies, as well as working through the Government Coordinating Council security partnership framework established in the National Infrastructure Protection Plan, TSA has established a Government coordination process that continues to mature and develop. TSA recognizes the need to specifically define roles and responsibilities with all freight rail security stakeholders, including industry and Federal, State, local, and tribal Governments. The appropriate document TSA is using to define roles and responsibilities, as well as describe communication methods and measurement efforts, is the Transportation Systems Sector Specific Plan modal annex.

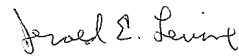
The DHS National Protection and Programs Directorate (NPPD) agrees that sharing assessments and information is a vital practice. NPPD will continue its efforts to appropriately coordinate with TSA.

**Appendix VII: Comments from the
Department of Homeland Security**

- 8 -

DHS appreciates the opportunity to review and comment on draft report GAO-09-243SU and we look forward to working with you on future homeland security issues.

Sincerely,



Jerald E. Levine

Director

Departmental DHS GAO/OIG Liaison Office

Appendix VIII: GAO Contact and Staff Acknowledgments

GAO Contact

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

Acknowledgments

In addition to the contact named above, Dawn Hoff, Assistant Director, and Chris Ferencik, Analyst-in-Charge, managed this assignment. Carissa Bryant, Jeremy Manion, and Gabriel Tonsil and made significant contributions to the work. William (Rudy) Chatlos assisted with design, methodology, and data analysis. Linda Miller provided assistance in report preparation, Tracey King provided legal support, and Greg Hanna provided expertise on freight rail issues.

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

