

December 2012

# PASSENGER RAIL SECURITY

## Consistent Incident Reporting and Analysis Needed to Achieve Program Objectives



G A O

Accountability \* Integrity \* Reliability

## Why GAO Did This Study

Terrorist attacks on foreign passenger rail systems, which include rail transit and intercity rail, have underscored the importance of collecting and analyzing security incident information to identify potential vulnerabilities. Within the federal government, TSA is the primary agency responsible for overseeing and enhancing passenger rail security, and has several programs to fulfill this responsibility. In 2008, TSA issued a regulation requiring U.S. passenger rail agencies to report all potential threats and significant security concerns to TSA, among other things. GAO was asked to assess the extent to which (1) TSA has overseen and enforced this reporting requirement and (2) TSA has analyzed passenger rail security incident information to identify security trends. GAO reviewed TSA policy documents, guidance, and incident data from January 2011 through June 2012, and interviewed federal officials and security officials from 19 passenger rail agencies. GAO selected these agencies, in part, because of their ridership volume. The results of these interviews are not generalizable but provide insights.

## What GAO Recommends

GAO recommends, among other things, that TSA (1) develop guidance on the types of incidents that should be reported, (2) enhance existing oversight mechanisms for compliance inspections and enforcement actions, (3) develop guidance to reduce errors from data entry problems, and (4) establish a process for regularly conducting trend analysis of incident data. TSA concurred and is taking actions in response.

View [GAO-13-20](#). For more information, contact Stephen M. Lord, (202)-512-4379, [lords@gao.gov](mailto:lords@gao.gov).

## PASSENGER RAIL SECURITY

### Consistent Incident Reporting and Analysis Needed to Achieve Program Objectives

## What GAO Found

The Transportation Security Administration (TSA) has inconsistently overseen and enforced its rail security incident reporting requirement because it does not have guidance and its oversight mechanisms are limited, leading to considerable variation in the types and number of incidents reported. Though some variation is expected in the number and type of incidents reported because of differences in rail agency size, location, and ridership, local TSA inspection officials have provided rail agencies with inconsistent interpretations of the reporting requirement. For example, local TSA officials instructed one rail agency to report all incidents related to individuals struck by trains. However, local TSA officials responsible for another rail agency said these incidents would not need to be reported as they are most often suicides with no nexus to terrorism. Providing guidance to local TSA inspection officials and rail agencies on the types of incidents that are to be reported could improve consistency across different TSA field offices. GAO also found inconsistency in TSA compliance inspections and enforcement actions because TSA has not utilized limited headquarters-level mechanisms as intended for ensuring consistency in these activities. TSA's rail security inspection policies do not specify inspection frequency but call for performing a "reasonable number" of inspections. However, 3 of the 19 rail agencies GAO contacted were not inspected from January 2011 through June 2012, including a large metropolitan rail agency, although local officials said it was unlikely that no incidents had occurred at that agency. Without inspections, TSA's assurance that rail agencies are reporting security incidents, as required, is reduced. In addition, TSA took enforcement action against an agency for not reporting an incident involving a knife, but did not take action against another agency for not reporting similar incidents, though the agency had been inspected. Enhancing headquarters-level mechanisms for overseeing inspection and enforcement actions in the field could help ensure more consistency in these activities and improve TSA's ability to use the information for trend analysis.

TSA has not conducted trend analysis of rail security information, and weaknesses in TSA's rail security incident data management system, including data entry errors, inhibit TSA's ability to search and extract information. Data entry errors occur in part because the guidance provided to officials responsible for entering incident information does not define the available data field options. Without the ability to identify information from the data, such as the number of incidents reported by incident type, TSA faces challenges determining if patterns or trends exist. Additional guidance for officials who enter the incident information could help to reduce data entry errors and improve users' ability to search and extract information from the system, ultimately improving TSA's ability to analyze the incident information. These weaknesses notwithstanding, TSA has made limited use of the incident information it has collected, in part because it does not have a systematic process for conducting trend analysis. TSA's purpose for collecting the rail security incident information was to allow TSA to "connect the dots" by conducting trend analysis. TSA has used the rail security incident information for situational awareness, but has conducted limited analysis of the information, missing an opportunity to identify any security trends or patterns in the incident information, or to develop recommended security measures to address any identified issues.

---

# Contents

---

Letter		1
	Background	8
	TSA Has Provided Inconsistent Oversight and Enforcement of the Passenger Rail Security Incident Reporting Requirement	11
	Incident Data and Process Limitations Hinder Trend Analysis	21
	Conclusions	28
	Recommendations for Executive Action	29
	Agency Comments and Our Evaluation	30
Appendix I	Influence of Foreign Attacks on Selected U.S. Rail Agencies' Security Measures	33
Appendix II	Selected Mechanisms Used to Gather Information on Lessons Learned from Passenger Rail Attacks and Share Rail Security Information	35
Appendix III	Objectives, Scope, and Methodology	38
Appendix IV	Summary of Recent Attacks against Foreign Passenger Rail Systems	43
Appendix V	Comments from the Department of Homeland Security	45
Appendix VI	GAO Contact and Staff Acknowledgments	48
Tables		
	Table 1: Selected Mechanisms Cited by Eight High-Volume Rail Agencies to Obtain and Share Rail Security Information	36
	Table 2: Passenger Rail Systems Interviewed	39

---

**Abbreviations**

AAR	Association of American Railroads
AFSD-I	assistant federal security director-inspection
CCTV	closed-circuit television
DHS	Department of Homeland Security
DOT	Department of Transportation
FRA	Federal Railroad Administration
FTA	Federal Transit Administration
I-STEP	TSA Intermodal Security Training and Exercise Program
MTI	Mineta Transportation Institute
PAG	TSA Transit Policing and Security Peer Advisory Group
PARIS	Performance and Results Information System
RSI-S	regional security inspector-surface
TSA	Transportation Security Administration
TSI-S	transportation security inspector-surface
TSOC	Transportation Security Operations Center

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.



G A O

Accountability \* Integrity \* Reliability

United States Government Accountability Office  
Washington, DC 20548

---

December 19, 2012

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

The Honorable Frank R. Lautenberg  
Chairman  
The Honorable Roger F. Wicker  
Ranking Member  
Subcommittee on Surface Transportation and Merchant Marine  
Infrastructure, Safety, and Security  
Committee on Commerce, Science, and Transportation  
United States Senate

Passenger rail systems are vital components of the nation's transportation infrastructure, encompassing rail mass transit (heavy rail and light rail), commuter rail, and intercity rail.<sup>1</sup> Terrorist attacks on passenger rail systems around the world—such as the March 2010 subway bombings in Moscow, Russia, and the July 2006 passenger train bombing in Mumbai, India, that resulted in 209 fatalities—highlight the vulnerability of these systems and demonstrate that even when security precautions are put into place, vulnerabilities remain. According to the Mineta Transportation Institute (MTI), from September 12, 2001, through December 31, 2011, there were 838 attacks worldwide on passenger rail

---

<sup>1</sup>Passenger rail systems consist of various mass transit and passenger rail transit systems. Transit rail is composed of heavy and light rail systems. Heavy rail is an electric railway that can carry a heavy volume of traffic, and is characterized by high speed and rapid acceleration, passenger rail cars operating singly or in multi-car trains on fixed rails, separate rights of way from which all other vehicular and foot traffic is excluded, sophisticated signaling, and high-platform loading. Most subway systems are considered heavy rail. Light rail systems typically operate passenger railcars singly (or in short, usually two-car trains) and are driven electrically with power being drawn from an overhead electric line. Commuter rail is characterized by passenger trains operating on railroad tracks and providing regional service, such as between a central city and its adjacent suburbs. Intercity rail is primarily provided by Amtrak. For purposes of this review we are using the term "passenger rail system" to include all of these different types of passenger rail transit systems.

---

systems, resulting in over 1,370 fatalities.<sup>2</sup> In the United States, passenger rail systems have received heightened attention as several alleged terrorists' plots have been uncovered, including plots against rail systems in the New York City and Washington, D.C., areas in 2009 and 2010, respectively. In addition, intelligence recovered from Osama bin Laden's compound indicates that U.S. rail systems were a suggested target as recently as February 2010, although there has been no indication of a specific or imminent threat to carry out such an attack. While there have been no terrorist attacks against U.S. passenger rail systems to date, the systems are vulnerable to attack in part because they rely on an open architecture that is difficult to monitor and secure because of its multiple access points; hubs serving multiple carriers; and, in some cases, no barriers to access. For example, in May 2011, an individual was able to walk the length of an underwater train tunnel between New York and New Jersey without being detected. Had this individual been a terrorist, he could have executed a disruptive and potentially damaging attack on this rail tunnel. Given the continued threat to passenger rail systems, such security breaches underscore the importance of tracking and analyzing security incident information to identify possible indicators or precursors of terrorist activity, as well as information on security vulnerabilities.

Securing the nation's passenger rail systems is a shared responsibility requiring coordinated action on the part of federal, state, and local governments; the private sector; and passengers who ride these systems. Day-to-day responsibility for securing passenger rail systems falls on passenger rail agencies themselves, local law enforcement, and often state and local governments that own a significant portion of the infrastructure. Within the federal government, the Department of Homeland Security's (DHS) Transportation Security Administration (TSA) is the primary federal agency responsible for overseeing security for these systems and for implementing programs to enhance their security.<sup>3</sup>

---

<sup>2</sup>The Mineta Transportation Institute database—Terrorist and Serious Criminal Attacks Against Public Surface Transportation—includes data on attacks against rail and other types of surface transportation. The Norman Y. Mineta International Institute for Surface Transportation Policy Studies was established by the Intermodal Surface Transportation Efficiency Act of 1991. Pub. L. No. 102-240, § 6024, 105 Stat. 1914 2188 (1991). The institute's transportation policy work is centered on, among other things, research into transportation security, planning, and policy development.

<sup>3</sup>The Department of Transportation's Federal Transit Administration also has responsibility for overseeing passenger rail agencies' system security plans. 49 C.F.R. pt. 659.

---

We have previously reported on federal and industry efforts to secure passenger rail systems and have made recommendations for strengthening these efforts.<sup>4</sup> DHS generally agreed with these recommendations and has taken actions to implement them. For example, in June 2009, we reported that TSA had taken some actions to implement a risk management approach but had not conducted a comprehensive risk assessment for mass transit and passenger rail that integrates threat, vulnerability, and consequence.<sup>5</sup> We recommended that TSA conduct a risk assessment that combines these three elements, which the agency could use to inform its security strategy. In response to our recommendation, in June 2010, TSA produced the Transportation Sector Security Risk Assessment, which assessed risk within and across the various aviation and surface transportation modes, including rail, and incorporated threat, vulnerability, and consequence assessments.

A key component of this shared responsibility for passenger rail security is ensuring that information on rail security threats and incidents is collected and analyzed effectively. As part of its rail security responsibilities, in 2008 TSA issued a regulation requiring U.S. passenger rail systems to report all potential threats and significant security concerns to TSA's Transportation Security Operations Center (TSOC), among other things.<sup>6</sup> The TSOC is a 24/7 operations center that serves as TSA's

---

<sup>4</sup>See, for example, GAO, *Rail Security: TSA Improved Risk Assessment but Could Further Improve Training and Information Sharing*, [GAO-11-688T](#) (Washington, D.C.: June 14, 2011); *Technology Assessment: Explosives Detection Technologies to Protect Passenger Rail*, [GAO-10-898](#) (Washington, D.C.: July 28, 2010); and *Transportation Security: Key Actions Have Been Taken to Enhance Mass Transit and Passenger Rail Security, but Opportunities Exist to Strengthen Federal Strategy and Programs*, [GAO-09-678](#) (Washington, D.C.: June 24, 2009).

<sup>5</sup>Threat is an indication of the likelihood that a specific type of attack will be initiated against a specific target or class of targets. Vulnerability is the probability that a particular attempted attack will succeed against a particular target or class of targets. Consequence is the effect of a successful attack.

<sup>6</sup>49 C.F.R. pt. 1580. These requirements generally apply to passenger rail carriers, including intercity passenger railroads, commuter railroads, and rail transit systems (subways and light rail), among others. The regulation also requires rail agencies to designate a rail security coordinator, and codifies TSA's authority to conduct security inspections of passenger rail agency property. 49 C.F.R. §§ 1580.201, 1580.5. This is the only rule that TSA has issued to date regarding passenger rail security. The Implementing Recommendations of the 9/11 Commission Act mandates TSA to develop and issue regulations for a public transportation security training program, among other things. Pub. L. No. 110-53, § 1408, 121 Stat. 266, 409 (2007). TSA stated it expects to issue a notice of proposed rulemaking for this program in 2013.

---

main point of contact for monitoring security-related incidents or crises in all modes of transportation. TSA's regulation is intended to provide the agency with essential information on passenger rail security incidents so that TSA can conduct comprehensive intelligence analysis, threat assessment, and allocation of security resources, among other things.<sup>7</sup> According to the regulation, potential threats and significant security concerns that must be reported to the TSOC encompass a variety of incidents and suspicious activities including bomb threats, indications of tampering with railcars, and other security breaches.<sup>8</sup>

You requested that we evaluate TSA's passenger rail security incident reporting process. Accordingly, this report addresses the following questions:

- To what extent has TSA overseen and enforced the passenger rail security incident reporting requirement?
- To what extent has TSA analyzed passenger rail security incident information to identify security trends and potential threats against passenger rail systems?

Appendix I of this report also includes information on how selected rail agencies applied lessons learned from foreign rail attacks to enhance their rail security measures. Appendix II includes information on key mechanisms rail agencies use to obtain rail security-related information.

To address these questions, we examined TSA's rail security incident reporting process. We reviewed the notice of proposed rulemaking and final rule that describe the purpose and justification of the incident reporting requirement, as well as relevant TSA policy documents, manuals, and guidance. To obtain rail industry perspectives on the rail security incident reporting process, we conducted visits at, or teleconferences with, 19 of the top 50 passenger rail systems across the

---

<sup>7</sup>71 Fed. Reg. 76,852, 76,876 (Dec. 21, 2006).

<sup>8</sup>49 C.F.R. § 1580.203(c). For the purposes of this report, we refer to potential threats and significant security concerns as rail security incidents.



---

nation, by passenger rail ridership.<sup>9</sup> See appendix III for a list of the 19 rail agencies we interviewed through our visits and teleconferences. We selected these 19 passenger rail systems to reflect varied levels of ridership and geographic dispersion. Because we selected a nonprobability sample of passenger rail agencies, the information obtained from these visits and interviews cannot be generalized to all rail agencies nationwide, but provided illustrative examples of the perspectives of passenger rail stakeholders about the rail security incident reporting process, and corroborated information we gathered through other means. Further, we interviewed rail industry representatives from the American Public Transportation Association<sup>10</sup> and the Association of American Railroads<sup>11</sup> to obtain their perspectives on rail security issues. We selected these associations because they represent the majority of the passenger and freight rail systems in the United States.

To assess the extent to which TSA has overseen and enforced the rail security reporting requirement, we interviewed officials from the selected rail systems discussed earlier on how they have implemented this requirement, including the guidance they have received from TSA. We interviewed TSA headquarters officials from the Compliance Programs Division within the Office of Security Operations and local TSA inspection officials from five TSA field offices regarding the guidance they provide to rail agencies on incident reporting and how they ensure rail agencies' compliance with the regulation. We selected these five field office locations because they had oversight responsibility for many of the rail

---

<sup>9</sup>The American Public Transportation Association compiled this ridership data from the Federal Transit Administration's National Transit Database. Ridership on rail transit systems in the District of Columbia and Puerto Rico is included in these statistics. Passenger rail ridership is calculated by the number of unlinked passenger trips. An unlinked passenger trip is defined as the number of passengers who board public transportation vehicles. Passengers are counted each time they board vehicles no matter how many vehicles they use to travel from their origin to their destination.

<sup>10</sup>The American Public Transportation Association represents the public transit industry. Its members serve more than 90 percent of persons using public transportation in the United States and Canada.

<sup>11</sup>The Association of American Railroads is a trade association whose membership includes freight railroads that operate 72 percent of the industry's mileage, employ 92 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.

---

agencies included in our scope. Because we selected a nonprobability sample of TSA's field offices and officials, the results from these interviews cannot be generalized to all field offices; however, the information we obtained provided us with an overview of the role of TSA surface inspectors in the rail incident reporting process and corroborated information we obtained through other sources. We also examined documentation on TSA's inspection processes for monitoring rail systems' compliance with the incident reporting requirement, including the *Transportation Security Inspector Inspections Handbook*, the *National Investigations and Enforcement Manual*, and the *Compliance Work Plan for Transportation Security Inspectors*.

In addition, we analyzed incident data from the TSOC's incident management database, known as WebEOC, for the period January 2011 through June 2012, to determine the number and types of passenger rail security incidents reported to the TSOC by rail agencies.<sup>12</sup> On the basis of information from and discussions with TSA officials related to the controls in place to maintain the integrity of TSA's incident data, we determined that the information in WebEOC was sufficiently reliable for the purposes of providing information on differences in the number and types of rail security incidents reported by selected rail agencies to the TSOC. However, we identified issues with data entry and data quality, which are discussed later in this report. In addition, we analyzed data from TSA's Performance and Results Information System (PARIS) for January 2011 through June 2012 on TSA's compliance inspections and all records related to enforcement actions taken under the passenger rail security incident reporting requirement.<sup>13</sup> We also evaluated TSA's efforts to oversee and enforce the incident reporting requirement against criteria in GAO's *Standards for Internal Control in the Federal Government*.<sup>14</sup>

---

<sup>12</sup>We chose January 2011 as the starting point for our analysis because it was 2 full years after the regulation became effective, which would allow rail agencies and TSA a period of adjustment. The regulation went into effect in December 2008. June 2012 was the end of our data collection period.

<sup>13</sup>All TSA inspection activities must be documented and entered into PARIS, along with any findings and actions taken. We chose January 2011 as the starting point for our analysis because it was 2 full years after the regulation became effective, which would allow rail agencies and TSA a period of adjustment.

<sup>14</sup>GAO, *Standards for Internal Control in the Federal Government*, [GAO/AIMD-00-21.3.1](#) (Washington, D.C.: Nov. 1, 1999).

---

To assess the extent to which TSA has analyzed rail security incident information, we interviewed TSA officials from the TSOC, the Office of Intelligence and Analysis, the Office of Security Operations, and the Office of Security Policy and Industry Engagement regarding their roles and responsibilities. We reviewed TSA documentation and analyses containing rail security incident information. We also examined the WebEOC incident management database to identify any database limitations that could present challenges for analyzing the incident information, and we discussed these limitations with TSA officials. We also interviewed officials from the rail agencies noted earlier about their views on the information and analyses they receive from TSA on rail security incidents.

To determine how selected rail agencies applied lessons learned from foreign rail attacks to enhance their rail security measures and how rail agencies obtain and share passenger rail security-related information, including information on lessons learned from foreign rail attacks, we interviewed security officials from selected passenger rail systems. During visits to passenger rail systems, we toured stations and other facilities such as control centers, and observed security practices. We also reviewed our prior reports on passenger rail security and information sharing as well as studies and reports conducted by outside organizations related to passenger rail, such as the DHS Office of the Inspector General. Appendix III provides more details on our objectives, scope, and methodology, including a list of the rail agencies we interviewed.

We conducted this performance audit from January 2012 through December 2012 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

---

## Background

As previously stated, TSA's 2008 regulation requires passenger rail agencies to report potential threats and significant security concerns to the TSOC.<sup>15</sup> According to the regulation, potential threats and significant security concerns (rail security incidents) include, but are not limited to, the following:

- 1) interference with the train or transit vehicle crew;
- 2) bomb threats, specific and non-specific;
- 3) reports or discovery of suspicious items that result in the disruption of rail operations;
- 4) suspicious activity occurring onboard a train or transit vehicle or inside the facility of a passenger railroad carrier or rail transit system that results in a disruption of rail operations;
- 5) suspicious activity observed at or around rail cars or transit vehicles, facilities, or infrastructure used in the operation of the passenger railroad carrier or rail transit system;
- 6) discharge, discovery, or seizure of a firearm or other deadly weapon on a train or transit vehicle or in a station, terminal, facility, or storage yard, or other location used in the operation of the passenger railroad carrier or rail transit system;
- 7) indications of tampering with passenger rail cars or rail transit vehicles;
- 8) information relating to the possible surveillance of a passenger train or rail transit vehicle or facility, storage yard, or other location used in the operation of the passenger railroad carrier or rail transit system;
- 9) correspondence received by the passenger railroad carrier or rail transit system indicating a potential threat to rail transportation; and
- 10) other incidents involving breaches of the security of the passenger railroad carrier or the rail transit system operations or facilities.

---

<sup>15</sup>49 C.F.R. § 1580.203. The rule also includes requirements that pertain exclusively to certain freight railroad carriers, rail hazardous materials shippers, and rail hazardous materials receivers, including a requirement that these entities report significant security concerns to the TSOC. 49 C.F.R. §§ 1580.100.111.

---

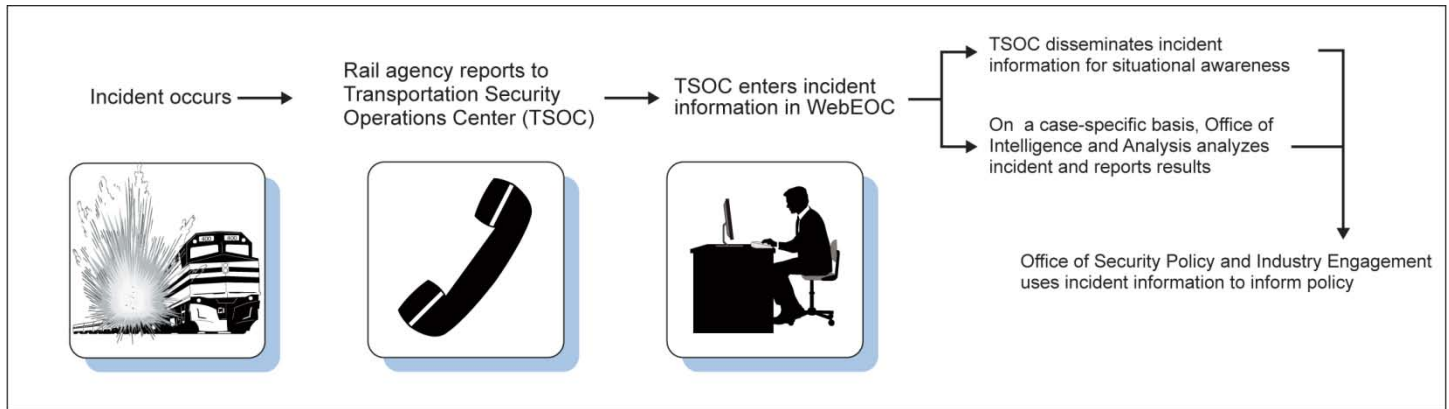
The regulation also authorizes TSA officials to view, inspect, and copy rail agencies' records as necessary to enforce the rail security incident reporting requirements.<sup>16</sup> This regulatory authority is supported by TSA policies and guidance, including the *Transportation Security Inspector Inspections Handbook*, the *National Investigations and Enforcement Manual*, and the *Compliance Work Plan for Transportation Security Inspectors*.

Within TSA, different offices have responsibilities related to implementing and enforcing the rail security incident reporting requirement. The TSOC, managed by TSA's Office of Law Enforcement/Federal Air Marshal Service, is the TSA entity primarily responsible for collecting and disseminating information about rail security incidents. Once notified of a rail security incident, TSOC officials are responsible for inputting the incident information into their incident management database known as WebEOC, and for disseminating incident reports that they deem high priority or significant to select TSA officials; other federal, state, and local government officials; and select rail agencies' law enforcement officials. TSA's Office of Intelligence and Analysis is responsible for analyzing threat information for all modes of transportation, including information related to passenger rail. TSA's Office of Security Policy and Industry Engagement is responsible for using incident reports and analyses, among other things, to develop strategies, policies, and programs for rail security, including operational security activities, training exercises, public awareness, and technology. Figure 1 shows the intended steps and responsibilities of TSA components involved in the rail security incident reporting process.

---

<sup>16</sup>49 C.F.R. § 1580.5

**Figure 1: The Intended Rail Security Reporting Process**



Source: GAO. Art Explosion (graphics).

TSA’s Office of Security Operations is responsible for overseeing and enforcing the incident reporting requirement. Responsible for managing TSA’s inspection program for the aviation and surface modes of transportation, the Office of Security Operations’ Surface Compliance Branch deploys approximately 400 transportation security inspectors-surface (TSI-S) nationwide.<sup>17</sup> The TSI-Ss are responsible for providing clarification to rail agencies regarding the incident reporting process highlighted in figure 1, and for overseeing rail agencies’ compliance with the reporting requirement by conducting inspections to ensure that incidents were properly reported to the TSOC. TSI-Ss also conduct assessments of surface transportation systems, including passenger rail systems, and oversee compliance with other applicable transportation security policies, directives, standards, and agreements. At the headquarters level within the Office of Security Operations, the Compliance Programs Division is responsible for assisting TSA management and surface inspection officials in the field by providing guidance and subject matter expertise in ensuring compliance by

<sup>17</sup>The surface transportation modes include mass transit and passenger rail, freight rail, highway and commercial vehicle, and pipeline. There are currently 68 TSA field offices under the Surface Compliance Branch. TSI-Ss report to assistant federal security directors-inspection (AFSD-I), who are responsible for all inspection, compliance, and enforcement activity in their areas of responsibility. Each office is led by a federal security director charged with the implementation of all field operational activities across all modes of transportation. For other transportation modes, in fiscal year 2012, TSA deployed 630 air cargo inspectors, and 958 aviation regulation inspectors.

---

regulated entities with security requirements. Six regional security inspectors-surface (RSI-S) within the Compliance Programs Division are responsible for providing national oversight of local surface inspection, assessment, and operational activities.

---

## TSA Has Provided Inconsistent Oversight and Enforcement of the Passenger Rail Security Incident Reporting Requirement

TSA has not provided consistent oversight of the implementation of the passenger rail security reporting requirement, leading to considerable variation in the types and number of rail security incidents reported. This variation is compounded by inconsistency in compliance inspections and enforcement actions, due in part to limited utilization of oversight mechanisms at the headquarters level.

---

## Variation in Implementation of the Reporting Requirement

Since the rail security incident reporting regulation went into effect in December 2008, local TSA inspection officials, who are the primary TSA points of contact for rail agencies, have not received clarifying guidance from TSA headquarters regarding how rail agencies should implement the reporting regulation. Although the regulation identifies 10 broad types of rail security incidents that must be reported to the TSOC, 7 of the 19 rail agencies we spoke with noted that there are several grey areas within these incident types that can be open to interpretation.<sup>18</sup> In the absence of clarifying guidance from TSA headquarters, local TSA inspection officials have provided rail agencies with inconsistent interpretations of the regulation's reporting requirements. Some variation is expected in the number of rail security incidents that rail agencies reported because of differences in agency size, geographic location, and ridership. For example, we analyzed incident data for 7 of the 19 rail agencies included in our review, and found that the number of incidents reported per million

---

<sup>18</sup>The seven rail agencies made these comments during open-ended discussions about the incident-reporting process in the course of our site visits and telephone interviews.

---

riders ranged from 0.25 to 23.15.<sup>19</sup> Inconsistent interpretation of the regulation by local TSA inspection officials has contributed to this variation.<sup>20</sup> For example, officials from one rail agency we spoke with had been told by their local TSA inspection officials that they were required to report all instances in which a person was hit by a train, because an individual cannot be struck by a train in the right of way without trespassing or breaching security. In contrast, officials from another rail agency told us that their agency does not report all of these incidents because they are most often intentional suicides that are unrelated to terrorism.<sup>21</sup> The local TSA inspection officials responsible for this agency agreed with this interpretation, noting that suicides generally have no nexus to terrorism.

Similarly, rail agencies may have received inconsistent feedback from their local TSA inspection officials about reporting incidents involving weapons. The regulation requires that rail agencies report incidents that involve the “discharge, discovery, or seizure of a firearm or other deadly weapon on a train or transit vehicle or in a station, terminal, facility, or storage yard, or other location used in the operation of the passenger railroad carrier or rail transit system.”<sup>22</sup> However, officials from one rail agency stated that if an individual is stopped for fare evasion and is subsequently found to be in possession of an illegal firearm, they would not report the incident to the TSOC because it is a local criminal incident unrelated to terrorism.<sup>23</sup> These officials explained that they would report only incidents that could have a nexus to terrorism, in part because reporting incidents that are unrelated to terrorism could reduce the quality

---

<sup>19</sup>This includes incidents reported to the TSOC from January 1, 2011, through December 31, 2011, and recorded in WebEOC. However, there are limitations and errors associated with these data, which are discussed in greater detail later in this report. Because of limitations associated with identifying the total number of incidents by agency, we limited this analysis to 7 of the 19 rail agencies that we included in our review. Ridership data for 2011 were provided by the American Public Transportation Association.

<sup>20</sup>For purposes of this report, “local TSA inspection officials” refers to TSI-Ss and AFSD-Is.

<sup>21</sup>While TSA has not provided written guidance on whether or not these types of incidents are to be reported, a senior TSA compliance official said that on the basis of his interpretation of the regulation, these types of incidents would not need to be reported.

<sup>22</sup>49 C.F.R. § 1580.203(c)(6).

<sup>23</sup>Officials noted that if the individual had several accomplices that were also in possession of weapons, the agency would report the incident to the TSOC.



---

of the data TSA collects. The local TSA inspection officials responsible for this agency have never found it to be in noncompliance for not reporting a weapon, tacitly approving of the agency's interpretation of the regulation. In contrast, officials at another rail agency said that they report all incidents related to weapons—regardless of their possible nexus to terrorism—because their local TSA inspection officials have instructed them that any firearm found in the system has to be reported. However, these officials stated that because of local gun laws, handguns are seized during the course of routine law enforcement activities, and are generally incidental to the original criminal offense. While they do report these local criminal incidents to the TSOC as directed by their local TSA inspection officials, the rail agency officials stated that it is unclear to them why it is necessary to do so if they have no nexus to terrorism. Clarification about which incidents should be reported could help address the confusion among rail agencies, and improve consistency in incident reporting.

Before the final rule was issued in November 2008, rail stakeholders raised concerns about the types of incidents required to be reported in commenting on the notice of proposed rulemaking. Specifically, some rail stakeholders noted when commenting on the proposed rule that the regulation's definition of reportable events was too broad and would result in an overload of information that would divert attention from truly significant threats and dilute the effectiveness of the reporting system.<sup>24</sup> Rail stakeholders requested that TSA clarify the reporting requirements, but in the preamble to the final rule, TSA stated that the agency would not further define or limit the scope of the reporting requirement, because doing so would reduce the data that TSA received, which could be used for broader trend analyses in order to anticipate or prevent an attack.<sup>25</sup> TSA has maintained this position, and as a result, has not developed clarifying guidance at the headquarters level regarding the reporting requirement.

---

<sup>24</sup>See 73 Fed. Reg. 72,130, 72,145 (Nov. 26, 2008).

<sup>25</sup>In the preamble to the final rule, TSA stated that "Detecting activities that may compromise transportation security entails piecing together seemingly unrelated incidents or observations and conducting analysis in context with information from other sources. However as the threat environment is dynamic and indicators of incident planning and preparation can change, TSA cannot provide a threshold for reporting events or a specific definition." 73 Fed. Reg. 72,130, 72,145 (Nov. 26, 2008).

---

However, local TSA inspection officials, headquarters level compliance officials, and rail agency officials that we interviewed stated that additional written guidance could help ensure that the regulation is implemented more consistently.<sup>26</sup> According to *Standards for Internal Control in the Federal Government*, information should be communicated in a way that allows officials to carry out their responsibilities.<sup>27</sup> In October 2011, we also reported that providing officials with guidance that contains specific criteria and definitions would provide greater assurance that decisions are made consistently.<sup>28</sup> For the aviation mode, TSA has established written guidance for reporting security incidents.<sup>29</sup> TSA's operational directive for reporting aviation security incidents includes attachments that, among other things, identify the types of incidents that are to be reported, based on the immediate security threat of different types of incidents. With regard to passenger rail, however, TSA has maintained the agency's position as detailed in the preamble to the final rule, as described above, and has not taken actions to develop clarifying guidance regarding the types of incidents that should be reported under the regulation. Providing similar guidance to local TSA inspection officials responsible for rail agencies could help to ensure that these officials are interpreting the regulation consistently across different field offices. These actions could also better position TSA to consistently collect rail security incident information, which may facilitate its efforts to conduct trend analysis and also help TSA to "connect the dots" to identify potential threats to passenger rail systems.

---

<sup>26</sup>Freight railroads are subject to the same TSA requirement to report rail security incidents, per 49 C.F.R. § 1580.105. Freight railroads' security professionals have raised similar concerns to TSA management about inconsistent guidance regarding the interpretation of the rule by local TSA surface inspection officials and the types of incidents that should be reported.

<sup>27</sup>[GAO/AIMD-00-21.3.1](#).

<sup>28</sup>See GAO, *Aviation Security: TSA Has Taken Steps to Enhance Its Foreign Airport Assessments, but Opportunities Exist to Strengthen the Program*, [GAO-12-163](#) (Washington, D.C.: Oct. 21, 2011).

<sup>29</sup>TSA, *Reporting Security Incidents to the Transportation Security Operations Center, Attachments 1-4*, OD-400-18-2D. This operational directive applies to TSA employees responsible for reporting aviation incidents. For passenger rail, regulated entities (rail agencies) are responsible for reporting rail security incidents.

---

## Inconsistent Compliance and Enforcement

TSA monitors passenger rail agency compliance with incident reporting requirements through compliance inspections and related enforcement activities at the local level, but TSA has not utilized its limited oversight mechanisms at the headquarters level as intended for ensuring consistency in these activities. Local TSA inspection officials conduct inspections of rail agencies to ensure compliance with the incident reporting requirement—that is, to ensure that rail agencies are properly reporting significant security concerns to the TSOC. In addition to monitoring compliance, inspections offer local TSA officials opportunities to provide rail agencies with feedback regarding their implementation of the regulation. TSA inspection officials also may take enforcement action against a rail agency that TSA finds to be not in compliance. Within TSA headquarters, the Compliance Programs Division within the Office of Security Operations is responsible for ensuring consistency in the application of all regulatory priorities that are to be implemented by the field and for monitoring and overseeing operational and field activities intended to support TSA's national rail security programs and objectives.

Our analysis of TSA's inspection data from January 1, 2011, through June 30, 2012, shows that the frequency of local TSA inspections of compliance with the reporting regulation varies among rail agencies. TSA's rail security inspection policies and guidance do not specify how often inspections should be conducted, instead recommending that inspections be driven by reportable events, with local discretion used to ensure a reasonable number of inspections are performed. According to senior TSA compliance officials, this means that inspections can be initiated in response to a particular incident that local TSA officials become aware of, as opposed to being scheduled at regular intervals. According to PARIS data, from January 1, 2011, through June 30, 2012, of the 19 rail agencies we spoke with, 7 agencies had been inspected at least 18 times, or an average of once per month. However, 3 agencies had not been inspected, including a large metropolitan rail agency.<sup>30</sup> Information in the text box below provides an example of this rail agency's experience with TSA compliance activities. Average monthly inspections for this time period ranged from about eight inspections to no inspections,

---

<sup>30</sup>We determined that the inspection data included in PARIS were sufficiently reliable to include in this report, but a senior TSA compliance official explained that some inspections may not have been consistently documented in PARIS. TSA's process for ensuring compliance with its PARIS documentation procedures was outside the scope of our review.

---

and there was also variation in the regularity with which inspections occur. For example, although 1 agency was inspected 4 times during the time period we reviewed, 3 of these inspections were conducted on the same day.<sup>31</sup> In contrast, another agency was inspected a total of 11 times, with each inspection occurring in a different month.

#### **TSA Had Not Inspected a Major Rail Agency**

On the basis of our review of the TSOC's database, we found that one major rail agency had not reported any incidents to the TSOC from January 1, 2011 through June 30, 2012. According to officials from this rail agency, the agency did not report any incidents because the rail agency had not clearly identified who in the agency was responsible for reporting incidents to the TSOC. Further, the local TSA inspectors responsible for this rail system had not conducted any compliance inspections to determine whether the system was meeting its requirement to report rail security incidents, according to PARIS inspection records. The regulation requires rail agencies to allow TSA inspectors to conduct inspections, copy records, and perform tests to ensure that rail agencies are meeting their rail security incident reporting responsibilities. Local TSA inspection officials told us, however, they did not have sufficient access to the rail agency's police records and personnel to complete these inspection activities and therefore were unable to determine whether rail security incidents have actually occurred in the system. Given the passenger volume of this rail system, the local TSA officials stated that it was highly unlikely that no rail security incidents had occurred. According to local news sources, several security incidents had occurred on the system during 2011 that, according to the regulation, should have been reported to the TSOC. For example, an Internet search we conducted in September 2012 indicated that in 2011, local news reported on a suspicious item found in one of the rail system's stations that resulted in a delay of service. Local TSA inspection officials stated that they did not pursue enforcement action against the rail system for incidents that should have been reported, nor did they request assistance from TSA's Surface Compliance Branch in obtaining access to the rail system's incident documentation. These local TSA inspection officials also explained that they are working on improving their relationship with the rail agency and their access to the agency's incident records.

---

<sup>31</sup>This could occur if a local inspection official created separate documentation in PARIS for individual incidents that were discussed with the rail agency on the same day.

---

TSA's policies also describe a variety of activities that may constitute an inspection. According to senior TSA compliance officials, these broad policies on how to conduct inspections contribute to inconsistent approaches across TSA field offices. For example, according to TSA policy, inspections could range from a phone call to the rail agency to inquire whether the agency reported a specific incident to more rigorous, regularly scheduled, on-site inspections of rail agencies' internal incident management systems. However, for an inspection official to inquire about whether an agency reported a specific incident by phone, that official must first become aware of the incident through other means, such as a media report, whereas on-site inspections could allow TSA inspection officials to identify incidents that did not result in media reports, but should have been reported to the TSOC under the regulation. Further, senior TSA compliance officials told us that some local TSA inspectors may be hesitant to conduct regular on-site inspections or find rail agencies not in compliance for incident reporting because doing so could make rail agencies less willing to participate in other important voluntary security activities, such as TSA's Baseline Assessment for Security Enhancement (BASE)<sup>32</sup> and the TSA-led Visible Intermodal Prevention and Response Program.<sup>33</sup> However, variations in the rigor and frequency of inspections highlight the need for enhanced oversight of these activities at the headquarters level to help ensure that rail agencies are reporting security incidents as required by the regulation.

In addition, TSA has inconsistently applied enforcement actions against rail agencies for not complying with the regulation. TSA's progressive enforcement policy includes the following steps, in order of severity, following a finding of not in compliance: (1) on-the-spot counseling, (2) administrative action—notice of noncompliance, and (3) civil penalty

---

<sup>32</sup>BASE reviews are non-regulatory security posture assessments. During a BASE review, surface inspectors, in coordination with the rail agency, assess the rail agency's overall security posture, focusing on the implementation and effectiveness of security plans, programs and measures, security gaps, and best practices. The results are used to inform the development of security programs and to determine priorities for allocating mass transit and passenger rail security grants.

<sup>33</sup>TSA's Visible Intermodal Prevention and Response Program works with local security and law enforcement officials to conduct a variety of security tactics to introduce unpredictability and deter potential terrorist actions, including random high-visibility patrols at passenger rail stations, and passenger and baggage screening operations involving specially trained behavior detection officers and explosive detection canine teams and technologies.

---

action.<sup>34</sup> In some cases, rail agencies have received a finding of not in compliance that resulted in on-the-spot counseling or a notice of noncompliance for failing to report certain types of incidents that other agencies may not report as a matter of standard practice, such as weapons discovered during the course of routine criminal activity. For example, one rail agency received a notice of noncompliance for failing to report an incident involving a knife that was discovered in an individual's possession after law enforcement officials intervened in a verbal altercation on a train. In contrast, as discussed above, officials from another rail agency said that they would not report routine criminal incidents involving weapons, including firearms and other deadly weapons such as knives, and had discussed this policy with their local TSA inspection officials. While the agency had been inspected, the local TSA officials had never issued a finding of noncompliance related to not reporting incidents involving weapons. TSA inspection officials have also taken an enforcement action against a rail agency for failing to report an incident that was not required to be reported. Specifically, one rail agency received a notice of noncompliance for failing to report a suspicious item discovered in the public area of one of its bus garages. However, according to a senior TSA compliance official, rail agencies are not required to report incidents involving buses or bus facilities, and therefore TSA officials should not take enforcement actions against rail agencies for failing to report bus incidents.

According to senior TSA compliance officials, inconsistent inspection and enforcement actions occur, in part because TSA has limited oversight mechanisms at the headquarters level, and has not utilized them as intended to monitor or oversee the rail security compliance and inspection

---

<sup>34</sup>TSA's enforcement framework proscribes progressively more punitive enforcement actions in response to repeated violations, failure of a regulated entity to take effective corrective action, flagrant violations, and violations that indicate chronic problems. According to TSA, for the enforcement framework to be effective, all inspections must be documented in PARIS. According to data in PARIS, for passenger rail agencies, TSA has taken 33 enforcement actions in the form of on-the-spot counseling, and issued four notices of noncompliance. TSA has never taken step 3 against a passenger rail agency in enforcing the rail security incident reporting regulation, according to PARIS data.

---

activities in the field.<sup>35</sup> *Standards for Internal Control in the Federal Government* provides that internal controls should be designed to ensure that ongoing monitoring occurs in the course of normal operations.<sup>36</sup> TSA established the regional security inspector-surface (RSI-S) position as a primary oversight mechanism at the headquarters level for monitoring compliance inspections and enforcement actions to help ensure consistency across field offices. However, according to TSA officials, the RSI-S is not part of the formal inspection process and has no authority to ensure that inspections are conducted consistently. The RSI-S also has limited visibility over when and where inspections are completed or enforcement actions are taken because TSA lacks a process to systematically provide the RSI-S with this information during the course of normal operations. As a result, TSA has limited assurance that the RSI-S will be able to provide oversight of local passenger rail inspection and enforcement activities.<sup>37</sup> For example, with regard to the situation discussed in the text box above, the RSI-S responsible for that rail agency was not aware that the agency had not reported any incidents to the TSOB and had never been inspected by the local TSA inspection officials. The text box below provides another example of the challenges that TSA faces in ensuring consistency across local TSA offices.

---

<sup>35</sup>A recent report from DHS's Office of the Inspector General found similar issues with TSA's oversight of aviation security incidents. Specifically, the report found that TSA did not have a process in place to ensure that all security breaches at airports are identified and reported, or to review security breach reports to identify reporting discrepancies among different airports. See DHS Office of Inspector General, *Transportation Security Administration's Efforts to Identify and Track Security Breaches at Our Nation's Airports* (Redacted), OIG-12-80 (Washington, D.C.: May 3, 2012).

<sup>36</sup>[GAO/AIMD-00-21.3.1](#).

<sup>37</sup>The freight rail industry has raised similar concerns to TSA management about the lack of an oversight role provided by the RSI-S in the regulatory inspection and compliance process.

---

---

### **TSA Efforts to Streamline Amtrak's Compliance Activities Face Challenges**

In 2010, Amtrak worked with an RSI-S to streamline the reporting and inspection process, but TSA has faced challenges implementing this process across all its field offices. As the only nationwide passenger rail agency, Amtrak has been regularly inspected by multiple TSA field offices in locations that Amtrak services.<sup>a</sup> According to Amtrak and TSA officials, these inspections are duplicative and cause confusion because incidents may be inspected for compliance by multiple TSA field offices, each with potentially different interpretations of the regulatory requirement. For example, one local TSA office found Amtrak to be not-in-compliance for not reporting an incident that another TSA office had told Amtrak did not need to be reported. To ensure that the regulation was being applied consistently throughout its operations, Amtrak notified the RSI-S of these inconsistencies between different field offices, and worked with the RSI-S to establish a centralized incident reporting and inspection process. Under this new process, according to Amtrak and TSA officials, all rail security incidents occurring on Amtrak nationwide should be reported to TSOC by Amtrak's National Communications Center in Philadelphia, Pennsylvania, rather than by the local Amtrak officials where the incident occurred. In addition, according to Amtrak and TSA officials, all TSA compliance inspections should be conducted by the local TSA field office in Philadelphia. According to these officials, the centralized reporting and inspection process has been implemented effectively by the Philadelphia field office. Specifically, between one and three times per month, a TSA official from the Philadelphia office checks compliance by randomly selecting security incidents from Amtrak's centralized incident monitoring system to determine whether they have been properly reported to the TSOC. However, although Amtrak and the RSI-S have implemented this reporting approach with the Philadelphia TSA office, other local TSA offices have continued to conduct compliance inspections of Amtrak. According to PARIS data, from January 2011 through July 2012, Amtrak was inspected 145 times. Of these, 116 were carried out by local TSA offices other than the Philadelphia office. According to senior TSA compliance officials, TSA headquarters has not taken actions to ensure that other field offices adhere to this centralized inspection approach, and TSA's mechanisms to monitor or oversee the rail security compliance and inspection activities in the field are limited.

<sup>a</sup>As the only nationwide passenger rail agency, Amtrak has a unique perspective on the differences between local TSA offices with regard to the reporting requirement. In a May 2012 hearing before the House Committee on Homeland Security, Amtrak testified that it has encountered difficulties over interpretation of regulations by different TSA field offices, and identified mission confusion and disconnects among offices and TSA headquarters regarding rail security incident reporting requirements.



---

In the absence of a process to systematically monitor the inspection and enforcement activities of TSA field offices, it is unlikely that the RSI-Ss or compliance officials at the headquarters level would become aware of inconsistencies in compliance and enforcement activities in the field, unless the inconsistencies were specifically brought to their attention. However, even when compliance officials have become aware of issues related to inconsistent application of compliance or enforcement measures in the field, according to senior TSA compliance officials, no action has been taken by the Office of Security Operations at the headquarters level to ensure consistency among field offices.<sup>38</sup> TSA inspection and compliance officials agreed that TSA could take steps to ensure more consistent application of compliance inspections and enforcement actions among TSA surface inspectors. By enhancing the existing oversight mechanisms at the headquarters level to systematically monitor and oversee compliance inspections and enforcement actions, as intended, TSA could improve its visibility over activities in the field, helping to ensure that local TSA inspection officials are consistently overseeing the regulatory reporting requirement. Such actions could further reduce inconsistency in the number and type of incidents that rail agencies report to the TSOC, which could improve TSA's ability to use the incident information for trend analysis to identify potential threats, as discussed below.

---

## Incident Data and Process Limitations Hinder Trend Analysis

TSA's incident management data system, known as WebEOC, has incomplete information, is prone to data entry errors, and has other limitations which inhibit TSA's ability to search and extract basic information. These weaknesses in WebEOC hinder TSA's ability to use rail security incident data to identify security trends or potential threats. In addition to these data weaknesses, TSA has conducted limited analysis of rail security incident information, in part because TSA does not have a systematic process for identifying trends or patterns in rail security incident information.

---

<sup>38</sup>Another way in which TSA headquarters could help to ensure consistency is through periodic conference calls that the Office of Compliance Programs hosts with local TSA inspection officials and RSI-Ss. However, according to senior TSA officials, passenger rail incident reporting issues have not been discussed during these calls.

---

## Incomplete Information

When TSA learns about an incident that may not have been properly reported to the TSOC (through a compliance inspection or other means), there is no established process to ensure that WebEOC is updated to include that incident.<sup>39</sup> As a result, WebEOC has incomplete incident information, which hinders TSA's ability to identify security trends and patterns. For example, over the course of 19 months, five similar incidents involving a suspicious item occurred in different stations of one rail agency. Although the rail agency did not report these incidents to the TSOC, the rail agency's internal intelligence group recognized a pattern, and developed an intelligence brief that it then disseminated to relevant rail stakeholders, including TSA. Upon receipt of this intelligence brief, local TSA inspection officials responsible for this rail agency issued a notice of noncompliance to the agency for not reporting two incidents highlighted in the brief.<sup>40</sup> In this case, the local TSA inspection official responsible for the agency reported these two incidents to the TSOC, but did not subsequently report the other three related incidents for inclusion in WebEOC.<sup>41</sup> Similarly, of the 18 findings of noncompliance that were a result of failure to report an incident, 13 were not subsequently reported to the TSOC. Because TSA has no established process to help ensure TSA inspection officials or rail agencies notify the TSOC or update WebEOC with incident information that was not properly reported, WebEOC does not contain a record of these unreported rail security incidents. *Standards for Internal Control in the Federal Government* calls for agencies to take actions to help ensure that data are complete and accurate.<sup>42</sup> Developing a process for ensuring the inclusion of incidents

---

<sup>39</sup>In addition to rail security incident reports provided to the TSOC directly from the rail agencies, WebEOC also contains incidents reported by TSA employees or the public, or incidents that TSOC officials became aware of as a result of media reports or other governmental incident management systems.

<sup>40</sup>The intelligence brief referred to similar incidents that had occurred previously, but did not provide specific details about those incidents.

<sup>41</sup>According to officials from the rail agency, they did not report four of these incidents to the TSOC because they believed that none of the individual incidents met the criteria for reporting—specifically, the incidents did not disrupt service, and the individual(s) who left the items were not required to breach security to do so. However, in issuing a notice of noncompliance, TSA stated that these incidents should have been reported. In response to TSA's notice of noncompliance, the agency stated that it had reported one of the incidents to the TSOC. According to TSA's investigation, however, the incident had been reported to local TSA inspection officials instead.

<sup>42</sup>[GAO/AIMD-00-21.3.1](#).

---

discovered during compliance inspections that were not immediately reported to the TSOC could provide TSA with a more comprehensive picture of security incidents to better position it to identify any trends or patterns.

---

## Data Entry Errors and Limitations

In addition, we identified data entry errors and limitations in WebEOC, which inhibit TSA's ability to search and extract certain information. Further, the guidance provided to officials responsible for entering incident information does not help prevent these errors because it allows for variation in the WebEOC data and assumes that the official responsible for entering the data fully understands the data entry options. As a result, the TSOC could not provide us with certain information about the rail security incident data, such as the number of incidents reported by incident type (e.g., suspicious item or bomb threat) or the total number of rail security incidents that have been reported to the TSOC.<sup>43</sup> Without the ability to identify this information on the number of incidents by type or the total number of incidents, TSA faces challenges determining if patterns or trends exist in the data, as the reporting system is intended to do. Additionally, because WebEOC does not contain a specific data field to identify the agency affected by the incident, TSA could not provide us with the total number of incidents reported by a particular agency.<sup>44</sup> Senior TSOC officials agreed with our findings and noted that these errors and limitations in WebEOC have complicated TSA's ability to use the data to identify security trends or potential threats. For example, TSA attempted to analyze the frequency of rail tunnel breaches occurring in the U.S. rail system, as directed by the conference report accompanying the DHS

---

<sup>43</sup>To conduct our analysis, we asked TSA to provide all passenger rail incidents reported to the TSOC from January 1, 2011, through June 30, 2012, as well as the total number of incidents reported by select rail agencies. In response to this request for data, TSA provided us with several inconsistent datasets from WebEOC, which officials attributed to differences in the way the data were searched and compiled from WebEOC.

<sup>44</sup>Such a data field would use a standard agency identifier, such as the agency name. (e.g., Amtrak or New York City Transit). Without such a field, identifying all the incidents reported by a specific agency requires TSOC officials to conduct a keyword search of the rail agency name, in the WebEOC incident narrative field, that accounts for any number of variations in the agency name, to include misspellings. For example, our review of WebEOC data revealed five potential key words for New York City Transit and Amtrak, including the misspelling "Amtrack." TSOC officials also noted that WebEOC lacks other specific data fields, such as incident location and severity, among others, that could help refine the data and improve the ability for it to be analyzed.

---

appropriations act for fiscal year 2012.<sup>45</sup> However, according to a senior TSA intelligence analyst, the rail security incident information from WebEOC was inadequate for conducting this analysis, and as a result, TSA had to request information from rail agencies and industry associations to complete the analysis.

We also found that WebEOC data entry errors occur, in part, because of problems in the data entry process and limitations in WebEOC, including inaccurate categorization of incident characteristics in key data fields, such as the “Incident Type” and “Type of Entry” fields.<sup>46</sup> For example, we analyzed 1 month of the data provided by TSA, which included a total of 152 passenger rail security incidents.<sup>47</sup> We reviewed the “Incident Type” data field for these incidents, and found that 106 (70 percent) were characterized as “Not Applicable” or “Other Rail Incidents.”<sup>48</sup> While this alone does not indicate that these incidents were mischaracterized, we found that 25 of these incidents should have been characterized under other available options, including “Firearm or Deadly Weapon,” “Bomb Threat,” or “Suspicious Activity,” among others. TSA officials agreed that the options for the “Incident Type” data field could often result in errors, and that these errors contributed to TSA’s inability to provide the number of security incidents reported by incident type.

With regard to the “Type of Entry” data field, TSA provided data extracted from WebEOC using the “Mass Transit” and “Rail” categories within this data field in response to our request for all of the passenger rail incidents reported from January 2011 through June 2012. However, because the WebEOC data entry options did not distinguish between passenger rail

---

<sup>45</sup>H.R. Rep. No. 112-331, at 973 (2011) (Conf. Rep.); S. Rep. No. 112-74, at 76 (2011).

<sup>46</sup>At the time of our review, the “Type of Entry” options included the following categories: cargo, highway, infrastructure, maritime, mass transit, natural disaster, notification, pipeline, postal, rail, and special event. The “Incident Type” entry options refer to the 10 incident types identified by the regulation, and are dependent on the selection under “Type of Entry.” Therefore, incidents that are improperly identified under “Type of Entry” cannot be correctly identified under “Incident Type.”

<sup>47</sup>The total number of incidents identified as “Mass Transit” or “Rail” for the month of August 2011 was 377. However, 60 percent of these entries were either related to freight rail or were batch e-mail notifications that contained multiple incidents, and were therefore excluded from our analysis.

<sup>48</sup>The “Incident Type” category includes data options that align with the incident type criteria identified by the regulation, as well as a “Not Applicable” category.

---

and freight rail, TSA could not provide a dataset that included only incidents reported by passenger rail agencies. Further, because TSA officials responsible for entering the incident data were not provided guidance that included definitions of the data entry options, incidents reported by the passenger rail agencies in our scope were sometimes categorized as “Mass Transit” and other times as “Rail.”<sup>49</sup> As a result of our review, TSOC officials recognized that the options available under the “Type of Entry” data field were a key limitation of the WebEOC system resulting in data entry errors. In July 2012, officials at TSOC removed “Rail” as an option within “Type of Entry,” and replaced it with two options—“Passenger Rail” and “Freight Rail.” TSOC officials also developed additional guidance for the individuals responsible for entering the data, which can be accessed directly from WebEOC. This guidance addresses the data entry options for the “Type of Entry” data field, providing definitions of each of the surface transportation modes included as options.

TSA’s actions to create new data entry options and guidance for the “Type of Entry” data field are positive steps toward improving the categorization of rail security incident data. However, TSOC officials have not taken similar actions to address issues that exist with other data fields in WebEOC, including the “Incident Type” data field. The WebEOC data entry guidance that TSA has provided officials in the TSOC for data fields other than “Type of Entry” does not help prevent data entry errors from occurring because it allows for variation in the WebEOC data and assumes that the official responsible for entering the data fully understands the data entry options. For example, the stated purpose of the guidance is to ensure that all necessary elements of an incident are captured “while maintaining each [official’s] unique style.” Further, the guidance states that the data fields such as “Incident Type” are “self-explanatory” and provides no additional information on how to enter the data or choose among different options.

We have previously reported on the importance of clear data entry guidance to help ensure that TSA is collecting consistent data that will

---

<sup>49</sup>In addition to these discrepancies, one option under “Type of Entry”—“Notifications”—was responsible for most of the incorrectly categorized incidents for the agencies in our scope. This discrepancy became clear when we compared agency-specific datasets (which were produced using keyword searches of the agency name) with the overall dataset that TSA provided.

---

allow the agency to better “connect the dots” with regard to potential terror threats to U.S. transportation systems.<sup>50</sup> Further, *Standards for Internal Control in the Federal Government* states that information should be communicated to officials within an agency in a way that allows them to carry out their responsibilities.<sup>51</sup> Additional guidance that contains clear definitions of data entry options could help TSA to reduce data entry errors in other data fields and improve users’ ability to search and extract basic information from the system, ultimately improving TSA’s ability to analyze the rail security incident information.

---

## Limited Use of Incident Information

The weaknesses in the incident information notwithstanding, TSA has made limited use of the rail security incident information it has collected from rail agencies, in part because it does not have a systematic process for conducting trend analysis. As a result, TSA is missing an opportunity to identify potential security trends and patterns in the incident information, and develop recommended security measures to mitigate threats, as intended. Although TSA does not have a systematic process for identifying trends and patterns using the WebEOC rail security incident information, opportunities exist to identify trends from the information, despite the data weaknesses discussed above. In one example, the freight rail industry, through the Railway Alert Network—which is managed by the Association of American Railroads, a rail industry group—identified a trend where individuals were reportedly impersonating federal officials. In coordination with TSA and FRA, the Railway Alert Network subsequently issued guidance to its member organizations designed to increase awareness among freight rail employees and provide descriptive information on steps to take in response. The Railway Alert Network identified this trend through analysis of incident reporting from multiple freight railroads. In each case, the incident had been reported by a railroad employee. These incidents had also been reported to the TSOC.

Similarly, in response to a specific request from freight rail stakeholders, TSA’s Office of Intelligence and Analysis, which is responsible for

---

<sup>50</sup>GAO, *Aviation Security: Efforts to Validate TSA’s Passenger Screening Behavior Detection Program Underway, but Opportunities Exist to Strengthen Validation and Address Operational Challenges*, [GAO-10-763](#) (Washington, D.C.: May 20, 2010).

<sup>51</sup>[GAO/AIMD-00-21.3.1](#).

---

analyzing threat information, used WebEOC incident information to identify the frequency and timing of shootings at freight trains.<sup>52</sup> However, other products developed by the Office of Intelligence and Analysis and other DHS components that address domestic rail security incidents do not contain trend analysis of reported rail security incidents and are instead generally limited to descriptions of specific incidents.<sup>53</sup> For example, TSA produces a series of periodic reports called the *Global and Regional Intelligence Digest* that provides descriptive reports of select transportation security incidents (for all transportation modes), with minimal accompanying analysis. Similarly, other products may contain intelligence information designed to inform rail stakeholders, but are based on sources other than the rail security incident data reported by rail agencies to the TSOC.<sup>54</sup> Senior TSA intelligence officials we spoke with agreed that TSA does not have a systematic process for analyzing the rail security incident information, and is not using the information to conduct long-term trend analysis, though agency officials said they would like to do so in the future.

In the absence of a systematic process for conducting trend analysis, TSA officials said that the agency primarily relies on internal TSA officials to notice trends when they receive daily incident report summaries from the TSOC, which are detailed summaries of the most significant incidents reported each day, across all modes of transportation. However, TSA officials said that the agency has not identified any trends in passenger rail incidents as a result of these summaries. As a result, officials from rail agencies we spoke with generally found little value in the reporting process, because it was unclear to them how, if at all, the information was being used by TSA to identify trends or threats that could help TSA and

---

<sup>52</sup>The TSOC is responsible for collecting the incident information from rail agencies and other sources, and providing this information to internal and external stakeholders. The Office of Security Policy and Industry Engagement is responsible for developing and recommending security measures or strategies to rail agencies.

<sup>53</sup>A senior TSA intelligence analyst explained that the Office of Intelligence and Analysis generally focuses on analyzing attacks that have occurred overseas. As noted earlier, there have been no successful attacks against rail in the United States. See appendix IV for descriptions of recent attacks on rail systems.

<sup>54</sup>These reports include, among others, the *Joint Information Bulletin*, produced by DHS and the Federal Bureau of Investigation, and *Mass Transit and Passenger Rail Threat Assessments*, produced by DHS's Office of Intelligence and Analysis, in coordination with TSA's Office of Intelligence and Analysis.

---

rail agencies develop appropriate security measures. The notice of proposed rulemaking,<sup>55</sup> final rule,<sup>56</sup> and the Privacy Impact Assessment associated with collecting the incident information in WebEOC state that TSA's purpose for collecting and maintaining the incident information is to help TSA "connect the dots." In these documents, the agency said it would "connect the dots" by pulling together seemingly disconnected or disparate reports of suspicious or unusual rail security incidents through trend analysis that may allow TSA to anticipate and prevent an attack, and determine whether to encourage or require rail agencies to implement particular security measures. Without a process for systematically conducting trend analysis of the rail security incident data, it will be difficult for TSA to use the incident data it collects from agencies. As a result, TSA may continue to miss opportunities to identify security trends, such as the freight rail security trend identified by the Railway Alert Network, or to develop recommended security measures.

---

## Conclusions

The foiled terrorist plots against the New York and Washington, D.C., passenger rail systems in 2009 and 2010, respectively, show the continued threat to passenger rail security and underscore the importance of tracking and analyzing security incident information to identify possible indicators or precursors of terrorist activity. TSA's incident reporting regulation, issued in 2008, was intended to allow TSA to "connect the dots" to identify significant incidents, and discern rail security threats and trends. However, TSA has not used the incident information as it was intended. Using the incident information to conduct trend analysis would better position TSA to anticipate a future attack, and encourage or require rail agencies to implement more targeted security measures. Key to the effectiveness of this effort is collecting consistent, accurate, and complete incident information from rail agencies. While some variation is expected among rail agencies in the number and types of rail security incidents reported, written guidance disseminated to rail agencies and local TSA inspection officials—clarifying the types of incidents that should be reported to the TSOC—and enhanced mechanisms for oversight of compliance and enforcement activities could help ensure that the regulation is implemented consistently. Such actions could also help improve consistency in TSA's compliance activities, thereby improving the

---

<sup>55</sup>71 Fed. Reg. 76,852, 76,865 (Dec. 21, 2006).

<sup>56</sup>73 Fed. Reg. 72,130, 72,145 (Nov. 26, 2008).



---

reporting process and facilitating TSA's ability to use the incident information for trend analysis that may identify potential threats.

In addition, incomplete information, data entry errors, and limitations in WebEOC hinder TSA's ability to use rail security incident data to identify security trends or potential threats. TSA has taken some steps toward addressing some of the weaknesses in WebEOC, but additional actions could improve the completeness and accuracy of the information in the database. A process for updating the database when incidents that had not previously been reported are discovered through compliance activities and additional guidance for TSOC officials who enter the information would help TSA to reduce data entry errors and improve users' ability to search and extract information from the system, ultimately improving TSA's ability to analyze the rail security incident information. The weaknesses in the incident information notwithstanding, without a systematic process in place for regularly conducting trend analysis, TSA has missed opportunities to use the data in its incident reporting system as it was intended—to identify trends or patterns in the incident information that could help TSA and rail agencies develop targeted security measures that could strengthen rail security.

---

## Recommendations for Executive Action

To help ensure that the rail security incident reporting process is consistently implemented and enforced, we recommend that the Administrator of TSA take the following two actions:

- develop and disseminate written guidance for local TSA inspection officials and rail agencies that clarifies the types of incidents that should be reported to the TSOC, and
- enhance and utilize existing oversight mechanisms at the headquarters level, as intended, to provide management oversight of local compliance inspections and enforcement actions.

To help fulfill TSA's stated purpose for collecting rail security incident information and improve the accuracy and completeness of the incident data in TSA's incident management system, WebEOC, we recommend that the Administrator of TSA take the following three actions:

- establish a process for updating the database when incidents that had not previously been reported are discovered through compliance activities;

- 
- develop guidance for TSOC officials that includes definitions of data entry options to reduce errors resulting from data entry problems; and
  - establish a systematic process for regularly conducting trend analysis of the rail security incident data, in an effort to identify potential security trends that could help the agency anticipate or prevent an attack against passenger rail and develop recommended security measures.

---

## Agency Comments and Our Evaluation

We provided a draft of this report to DHS for comment. In written comments received December 4, 2012, DHS concurred with the recommendations and identified actions taken, planned, or under way to implement the recommendations. DHS's written comments are summarized below and reproduced in appendix V. The Department of Transportation's Director of Audit Relations stated in an e-mail received on December 6, 2012, that the department had no comments on the report. Amtrak's audit liaison stated in an email received on November 16, 2012, that Amtrak had no comments on the report.

In its written comments, DHS concurred with our recommendation that TSA develop and disseminate written guidance for local TSA inspection officials and rail agencies that clarifies the types of incidents that should be reported to the TSOC. DHS stated that TSA's Office of Security Operations and its Office of Security Policy and Industry Engagement will work together to develop written guidance for passenger rail agencies clarifying the types of incidents that should be reported to the TSOC. TSA plans to disseminate the guidance to passenger rail agencies. If implemented, these actions would address our recommendation and could help reduce confusion among rail agencies and improve consistency in incident reporting.

In response to our recommendation that TSA enhance and utilize existing oversight mechanisms at the headquarters level, as intended, DHS concurred with the recommendation and stated that while several mechanisms and layers are in place for oversight and management of local inspection and enforcement actions, TSA recognizes that there are opportunities for improving oversight. According to DHS, existing oversight mechanisms include RSI-Ss, who serve as technical specialists, oversee and implement transportation security policy and programs, and conduct field office audits and visits, among other things. DHS also stated that its Office of Chief Counsel coordinates enforcement actions with RSI-Ss, local field offices, TSA's Office of Compliance Programs, and TSA's

---

Office of Security Policy and Industry Engagement. DHS stated that to improve headquarters oversight, RSI-Ss have recently been granted case review privileges in PARIS—which is used to record all TSA inspection activities—along with any findings and actions taken. DHS stated that this will allow the RSI-Ss greater visibility on all surface inspections, investigations, and recommendations for enforcement actions entered into PARIS by enabling the RSI-Ss to provide written recommendations in PARIS prior to inspection approval. Because RSI-Ss have recently been granted this access, it is too soon to determine the extent to which this action will address our recommendation.

In response to our recommendation that TSA establish a process for updating its WebEOC database when incidents that had not been previously reported are discovered through compliance activities, DHS concurred and stated that TSA is currently establishing a business process to ensure the relevant databases are complete. According to DHS, the WebEOC system will be adjusted to permit inputting of records that are discovered through compliance activities. We will continue to monitor the agency's efforts to implement our recommendation.

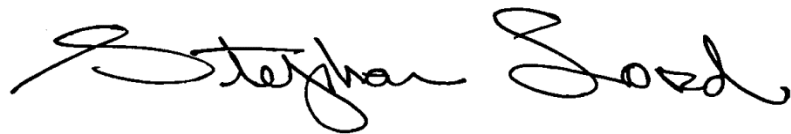
DHS also concurred with our recommendation that TSA develop guidance for TSOC officials that includes definitions of data entry options to reduce errors resulting from data entry problems. DHS stated that the TSOC had completed implementing this recommendation by updating the guidance with respect to input options. However, the updated guidance that TSA sent to us clarifies that incident logs in WebEOC need to indicate that an incident was reported by phone. The guidance does not provide definitions for data entry options, as we recommended, and we therefore continue to believe that additional guidance is necessary for the officials responsible for inputting the incident information into WebEOC.

In response to our recommendation that TSA establish a systematic process for regularly conducting trend analysis of the rail security incident data, in an effort to identify potential security trends, DHS concurred and stated that TSA will develop a process to review suspicious activities and incidents in the mass transit and passenger rail areas in order to identify trends that might represent a threat to transportation. We will continue to monitor the agency's efforts to implement our recommendation.

---

We are sending copies of this report to the Secretaries of Homeland Security and Transportation, the TSA Administrator, Amtrak, appropriate congressional committees, and other interested parties. In addition, this report is available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at (202) 512-4379 or [lords@gao.gov](mailto:lords@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 acknowledged in appendix VI.

A handwritten signature in black ink that reads "Stephen Lord". The signature is written in a cursive, flowing style.

Stephen M. Lord  
Director, Homeland Security  
and Justice Issues

---

# Appendix I: Influence of Foreign Attacks on Selected U.S. Rail Agencies' Security Measures

---

Officials we met with from eight high-volume rail agencies generally stated that foreign rail attacks (such as those described in appendix IV) served as potent reminders of potential terror threats against rail, but they did not lead the rail agencies to make significant changes in their security measures.<sup>1</sup> Nonetheless, agencies have used these incidents to inform security enhancements. Specifically, these agencies reported making changes to their security measures, in part as a result of lessons learned from foreign attacks.<sup>2</sup> These changes were related to:

- *Public awareness campaigns.* These include publicity posters and announcements over public address systems within rail stations that alert passengers and rail agency employees to report suspicious items or behaviors to police. For example, officials from one rail agency we spoke with reported making changes to its public awareness campaign following the attacks in Madrid and London. These changes included instituting a regional transit security awareness program, including periodic audio announcements reminding passengers to be aware of potential threats, in coordination with the Federal Transit Administration's Transit Watch Program. Other rail agencies reported that the attacks described in appendix IV emphasized the importance of having informed riders that can act as a "force multiplier" when it comes to noticing suspicious activity.
- *Armed mobile tactical teams.* These are police teams similar to SWAT teams that patrol rail systems or that are intended for rapid deployment in the event of a terror attack or related incident. Officials from one high-volume rail agency reported that the 2008 attack in Mumbai led it to immediately increase training in responding to "active shooter" scenarios by its existing mobile tactical teams. Officials from other high-volume rail agencies we interviewed also reported that they

---

<sup>1</sup>The high-volume passenger rail agencies we interviewed were: Amtrak; the New York City Metropolitan Transit Authority; New York-New Jersey Port Authority; New Jersey Transit; Washington Metropolitan Area Transit Authority; Chicago Transit Authority; Metra; and San Francisco Bay Area Rapid Transit. We also interviewed municipal police departments that provide security for two of these transit systems, including the New York Police Department Transit Bureau and the Chicago Police Department Public Transportation Section.

<sup>2</sup>For additional information on rail security measures implemented by TSA and rail agencies, see GAO, *Transportation Security: Key Actions Have Been Taken to Enhance Mass Transit and Passenger Rail Security, but Opportunities Exist to Strengthen Federal Strategy and Programs*, [GAO-09-678](#) (Washington, D.C.: June 24, 2009).

established mobile tactical teams or increased the training of their existing patrols following the 2008 Mumbai attacks.

- *Motorized emergency response vehicles.* These are small battery-operated vehicles intended to help first responders reach injured or stranded passengers when they cannot be quickly reached by a rescue train (if, for example, rails have been damaged by a terror blast or electrical outage). Officials from one agency we interviewed reported that it deployed these response vehicles directly in response to lessons learned from the London attack, during which first responders used such vehicles to rescue injured Underground rail passengers.
- *Closed-circuit television (CCTV).* CCTV refers to a visible or covert video system intended for only a limited number of viewers. In CCTV, the picture is viewed or recorded, but not broadcast. According to officials from two high-volume rail agencies we interviewed, the July 2005 attacks in London demonstrated the utility of CCTV coverage for forensic investigation. A United Kingdom government analysis reported that the cameras helped police determine the identity of the bombers. Officials from four high-volume rail agencies we interviewed stated that while they increased the number of CCTV cameras in their rail systems, this did not occur immediately following the London attacks. Rather, the London attacks reinforced the importance of CCTV camera coverage as a key security measure.

---

# Appendix II: Selected Mechanisms Used to Gather Information on Lessons Learned from Passenger Rail Attacks and Share Rail Security Information

---

The Transportation Security Administration (TSA) and officials from eight high-volume passenger rail agencies we interviewed identified several different mechanisms they use to obtain and share passenger rail security-related information, including information on lessons learned from foreign rail attacks (such as those described in appendix IV) and security measures implemented or considered by other U.S. rail stakeholders.<sup>1</sup> Many of these mechanisms have also been discussed in our previous reports on information sharing and rail security issues.<sup>2</sup> The key mechanisms that officials from the eight high-volume rail agencies we interviewed cited using to obtain and share passenger rail security-related information are summarized in table 1.

---

<sup>1</sup>These mechanisms were cited by TSA and high-volume passenger rail stakeholders or by rail security entities associated with them (i.e., police departments that are part of a rail system, or that provide policing for one of the high-volume systems that we interviewed). The high-volume passenger rail agencies we interviewed were: Amtrak; the New York City Metropolitan Transit Authority; New York-New Jersey Port Authority; New Jersey Transit; Washington Metropolitan Area Transit Authority; Chicago Transit Authority; Metra; and San Francisco Bay Area Rapid Transit. We also interviewed municipal police departments that provide security for two of these transit systems, including the New York Police Department Transit Bureau and the Chicago Police Department Public Transportation Section.

<sup>2</sup>Our prior work on information sharing with private and public security stakeholders has shown that security-related information sharing continues to be a challenge for the federal government. See, for example, GAO, *Transportation Security Information Sharing: Stakeholders Generally Satisfied but TSA Could Improve Analysis, Awareness, and Accountability*, [GAO-12-44](#) (Washington, D.C.: Nov. 21, 2011); *Public Transit Security Information Sharing: DHS Could Improve Information Sharing through Streamlining and Increased Outreach*, [GAO-10-895](#) (Washington, D.C.: Sept. 22, 2010); and *Transportation Security: Key Actions Have Been Taken to Enhance Mass Transit and Passenger Rail Security, but Opportunities Exist to Strengthen Federal Strategy and Programs*, [GAO-09-678](#) (Washington, D.C.: June 24, 2009).

**Appendix II: Selected Mechanisms Used to Gather Information on Lessons Learned from Passenger Rail Attacks and Share Rail Security Information**

**Table 1: Selected Mechanisms Cited by Eight High-Volume Rail Agencies to Obtain and Share Rail Security Information**

<b>Mechanism</b>	<b>Mechanism description</b>
TSA Transit Policing and Security Peer Advisory Group (PAG)	<p>The PAG is a monthly TSA-sponsored forum consisting of transit police chiefs and security directors from 21 major transit agencies in the country. The PAG holds regular monthly teleconferences and meetings, where participants discuss issues of concern to them, including security-related developments, and lessons learned from ongoing security processes.</p> <p>Officials from three of the eight rail agencies we interviewed described the PAG as useful for police and security officials to exchange information on rail security measures implemented by similar rail agencies, and to get to know one another.</p>
TSA transit community information-sharing call	<p>TSA facilitates monthly teleconferences with over 300 rail stakeholders invited to participate. These calls generally include an unclassified threat briefing conducted by the TSA Office of Intelligence and Analysis, TSA announcements, and presentations by rail agency officials on security best practices.</p> <p>Officials from one rail agency cited these calls as a useful way to discuss security-related information with a large number of interested stakeholders on a regular basis, thus improving their preparedness and situational awareness. However, another rail agency official noted that rail agencies may be hesitant to share their sensitive security practices in a teleconference setting.</p>
DHS's Homeland Security Information Network (HSIN)	<p>HSIN is an access-restricted website available to rail and other transportation stakeholders. It is intended to provide searchable information to transportation-related entities including passenger rail.</p> <p>Officials from one rail agency cited HSIN as a useful resource to improve knowledge of rail-related events both in the United States and overseas.</p>
Public Transportation Information Sharing and Analysis Center (PT-ISAC) <sup>a</sup>	<p>Administered by the American Public Transportation Association, and in collaboration with TSA, the Federal Transit Administration (FTA), and the Association of American Railroads, the PT-ISAC is a 24/7 information center that collects, analyzes, and distributes security- and threat-related information to transportation entities from the federal government and open sources. For example, daily unclassified e-mail bulletins known as the <i>Transit and Rail Intelligence Awareness Daily</i> (TRIAD) are sent to subscribers summarizing and analyzing security information, news, threats, and potential vulnerabilities within the transportation sector.</p> <p>Officials from one rail agency we interviewed noted that information and analyses sent out by PT-ISAC, including TRIAD messages, have been particularly helpful for understanding rail security threats and incidents overseas.</p>
The International Working Group on Land Transport Security	<p>The working group consists of 20 countries and two observer organizations that meet annually to share best practices on surface transportation security. For example, the 2010 annual conference culminated in the completion of 71 "smart" rail security practices. TSA participates as the lead federal agency for the United States. TSA states that its participation permits it to identify effective rail security best practices and counterterrorism measures for potential integration domestically and states that it shares the information acquired through a variety of mechanisms, such as the monthly PAG and other teleconferences with rail stakeholders.</p>
FTA e-mail alerts	<p>The lead emergency coordinator at FTA disseminates rail security information to approximately 500 individuals and organizations, including public transit agencies; federal, state, and local agencies; fusion centers; and law enforcement. Information is disseminated over e-mail and includes breaking news alerts, updates on incidents affecting rail operations, and intelligence information.</p> <p>One rail agency official noted that he received most of his security-related information from the FTA e-mail alerts.</p>
TSA/FTA Transit Security and Safety Roundtables	<p>TSA and FTA host roundtables with the nation's largest passenger rail agencies to discuss security challenges, terrorism prevention, and efforts to develop effective risk mitigation and security enhancements. These roundtables were formerly held twice a year, but will now be held annually, according to TSA officials. The meeting scheduled for 2012 has been postponed as FTA and TSA reconfigure the event.</p> <p>Several rail agencies described these roundtable discussions as useful for getting to know other rail security officials and keeping current on situational awareness and potential security threats.</p>



**Appendix II: Selected Mechanisms Used to Gather Information on Lessons Learned from Passenger Rail Attacks and Share Rail Security Information**

Mechanism	Mechanism description
Other rail agencies	<p>Some rail agencies and their associated police forces have their own internal intelligence officers or departments that are responsible for analyzing international and domestic intelligence to identify potential threats or lessons learned from foreign attacks. For example, the New York Police Department maintains 11 overseas offices for the purposes of gathering information on potential terror threats. The New York Police Department also maintains a restricted access website, The Shield, which makes available to rail and other security officials a wide variety of rail and other terror-related information and analysis. As another example, Boston’s Massachusetts Bay Transportation Authority sends out analyses and information to other rail agencies.</p> <p>Both of these mechanisms—internal intelligence officers and the restricted access website—were cited by rail agencies we interviewed as providing useful information about foreign rail attacks and for keeping aware of rail-related security issues.<sup>b</sup></p>
Industry websites and related information distribution mechanisms	<p>Passenger rail industry organizations such as the American Public Transportation Association maintain websites to share information directly with public transit agencies. The American Public Transportation Association maintains a website with detailed security- and safety-related rail standards and recommended practices in 29 areas, including perimeter and station security.</p> <p>Officials from one rail agency cited the association’s online resources as helpful for identifying standards for security.</p>
Baseline Assessment for Security Enhancement (BASE) review process	<p>TSA’s BASE reviews provide periodic assessments of how well rail systems are meeting rating criteria related to rail security. BASE has 17 security and emergency management action items described by TSA as forming the foundation of an effective security program. These include topics such as agency security plans and training, public outreach efforts, and background checks. The BASE assessment analyzes the security program for each transit system and identifies vulnerabilities. Participation in a BASE assessment is voluntary. According to TSA, the agency is updating the BASE assessment criteria to make the assessment more robust.</p> <p>Officials from two rail agencies found BASE assessments to be useful by alerting them to needed improvements in their security-related processes or because they provide a minimum standard for security measures.</p>
TSA Intermodal Security Training and Exercise Program (I-STEP)	<p>Through I-STEP, TSA employs multiphased workshops, tabletop exercises, and “lessons learned” working groups to integrate mass transit and passenger rail agencies with regional law enforcement and emergency response partners to expand and enhance coordinated deterrence and incident management capabilities.</p> <p>Officials from two rail agencies cited I-STEP as useful for improving security processes and awareness.</p>

Source: GAO analysis of DHS, Department of Transportation, American Public Transportation Association, and rail agency information.

<sup>a</sup>The PT-ISAC was created under the direction of the Department of Transportation (DOT) in 2003 and is funded by TSA via DOT’s FTA. According to the American Public Transportation Association, its members serve more than 90 percent of persons using public transportation in the United States and Canada. The American Public Transportation Association is responsible for validating PT-ISAC membership. For more information on PT-ISAC, see GAO, *Transportation Security Information Sharing: Stakeholders Generally Satisfied but TSA Could Improve Analysis, Awareness, and Accountability*, GAO-12-44 (Washington, D.C.: Nov. 21, 2011) and GAO, *Public Transit Security Information Sharing: DHS Could Improve Information Sharing through Streamlining and Increased Outreach*, GAO-10-895 (Washington, D.C.: Sept. 22, 2010).

<sup>b</sup>We have previously reported in GAO-10-895 that public transit agencies may receive unclassified security-related information from other public transit agencies on an ad-hoc basis. For example, a large public transit agency may pass along security-related information to a smaller agency in the same geographic region, or security officials at one agency may receive information from officials at other agencies around the country through informal networks.

---

# Appendix III: Objectives, Scope, and Methodology

---

This report addresses the following questions:

- To what extent has the Transportation Security Administration (TSA) overseen and enforced the passenger rail security incident reporting requirements?
- To what extent has TSA analyzed passenger rail security incident information to identify security trends and potential threats against passenger rail systems?

Appendix I of this report also includes information on how selected rail agencies applied lessons learned from foreign rail attacks to enhance their rail security measures. Appendix II includes information on key mechanisms rail agencies use to obtain rail security-related information.

To address these questions, we examined TSA's rail security incident reporting process. We focused on TSA's regulation for rail security incident reporting, which requires passenger rail agencies to report rail security incidents to the Transportation Security Operations Center (TSOC). We reviewed the notice of proposed rulemaking and final rule that describe the purpose and justification of the incident reporting requirement, as well as TSA policy documents, manuals, and guidance concerning the rail security incident reporting process. We also interviewed cognizant TSA officials at headquarters and in the field regarding their roles in the incident reporting process. To obtain rail industry perspectives on the rail security incident reporting process, we conducted visits at, or teleconferences with, 19 of the top 50 passenger rail systems across the nation, by passenger rail ridership.<sup>1</sup> See table 2 for a list of passenger rail systems we interviewed. We selected these passenger rail systems to reflect varied levels of ridership and geographic dispersion. Because we selected a nonprobability sample of passenger rail systems, the information obtained from these visits and interviews cannot be generalized to all rail systems nationwide. However, we determined that the selection of these rail systems was appropriate for

---

<sup>1</sup>The American Public Transportation Association compiled these ridership data from the Federal Transit Administration's National Transit Database. Ridership data on rail transit systems in the District of Columbia and Puerto Rico are included in these statistics. Passenger rail ridership is calculated by the number of unlinked passenger trips. An unlinked passenger trip is defined as the number of passengers who board public transportation vehicles. Passengers are counted each time they board vehicles no matter how many vehicles they use to travel from their origin to their destination.

our design and objectives and that the selection would provide valid and reliable evidence. The information we obtained provided illustrative examples of the perspectives of various passenger rail stakeholders about the rail security incident reporting process, and corroborated information we gathered through other means. Further, we interviewed rail industry representatives from the American Public Transportation Association and the Association of American Railroads to obtain their perspectives on rail security issues. We selected these associations because they represent the majority of the passenger and freight rail systems in the United States.

**Table 2: Passenger Rail Systems Interviewed**

<b>Passenger rail system</b>	<b>Urban area served</b>
Amtrak	Nationwide
Bay Area Rapid Transit (BART)	San Francisco—Oakland, California
Bi-State Development Agency	St. Louis, Missouri
CALTRAIN	San Francisco and San Jose, California
Charlotte Area Transit System	Charlotte, North Carolina
Chicago Transit Authority (CTA)	Chicago, Illinois
Greater Cleveland Regional Transit Authority	Cleveland, Ohio
Denver Regional Transportation District	Denver, Colorado
Maryland Transit Administration (MTA)	Baltimore, Maryland and Washington, D.C.
Metra Commuter Rail	Chicago, Illinois
New Jersey Transit	Newark, New Jersey—New York, New York
New York Metropolitan Transit Authority (MTA)	New York, New York
Northern Indiana Commuter Transportation District	Chicago, Illinois
Port Authority of Allegheny County	Pittsburgh, Pennsylvania
Port Authority Trans Hudson (PATH)	New York, New York—New Jersey
San Francisco Municipal Railway (Muni)	San Francisco, California
Utah Transit Agency	Salt Lake City, Utah
Virginia Railway Express (VRE)	Washington, D.C.
Washington Metropolitan Area Transit Authority (WMATA)	Washington, D.C.

Source: GAO.

To assess the extent to which TSA has overseen and enforced the rail security reporting requirement, we interviewed officials from the selected rail systems discussed earlier on how they have implemented this requirement, including the guidance they have received from TSA on the types of incidents to report to the TSOC. We interviewed TSA headquarters officials from the Compliance Programs Division within the Office of Security Operations and local TSA officials from five field offices, including transportation security inspectors-surface (TSI-S) and assistant federal security directors-inspections (AFSD-I), regarding the guidance they provide to rail agencies on incident reporting and how they ensure rail agencies' compliance with the regulation. We selected these five field office locations because they had oversight responsibility for many of the rail agencies included in our scope. We also interviewed one TSA regional security inspector-surface (RSI-S) regarding his role in the rail security incident reporting process.<sup>2</sup> Because we selected a nonprobability sample of TSA's field offices and officials, the results from these interviews cannot be generalized to all TSA field offices; however, the information we obtained provided us with an overview of the role of TSA surface inspectors in the rail incident reporting process and corroborated information we obtained through other sources. We examined documentation on TSA's inspection processes for monitoring rail systems' compliance with the incident reporting requirement, including the *Transportation Security Inspector Inspections Handbook*, the *National Investigations and Enforcement Manual*, and the *Compliance Work Plan for Transportation Security Inspectors*. We also reviewed a TSA operational directive related to reporting aviation security incidents to TSA.

We obtained incident data from the TSOC's incident management database, known as WebEOC, for the period January 2011 through June 2012.<sup>3</sup> We reviewed the data to determine the number and types of passenger rail security incidents reported to the TSOC by rail agencies. We also analyzed the data to identify differences in the number or types of rail security incidents reported by rail agencies of comparable size and volume. As part of this work, we assessed the reliability of data in

---

<sup>2</sup>There are six RSI-Ss located throughout the country.

<sup>3</sup>We chose January 2011 as the starting point for our analysis because it was 2 full years after the regulation became effective, which would allow rail agencies and TSA a period of adjustment. The regulation went into effect in December 2008. June 2012 was the end of our data collection period.

WebEOC by conducting visits to the TSOC and interviewing TSOC officials to discuss their role in incident reporting and the mechanisms in place to ensure data quality. We also reviewed WebEOC documentation to identify how passenger rail security incident data are collected and managed, and how data quality is ensured. While we determined that the information in WebEOC was sufficiently reliable for the purposes of providing information on differences in the number and types of rail security incidents reported by selected rail agencies to the TSOC, we identified issues with data entry and data quality, which are discussed in this report. In addition, we obtained data from TSA's Performance and Results Information System (PARIS) for January 2011 through June 2012 on TSA's compliance inspections and all records related to enforcement actions taken under the passenger rail security incident reporting requirement.<sup>4</sup> We analyzed the data to identify the content and frequency of TSA inspections conducted and enforcement actions taken under the incident reporting regulation. We ascertained the reliability of compliance data derived from PARIS by interviewing TSA officials from the Compliance Programs Division and reviewing documentation on controls implemented to ensure the integrity of the data in PARIS, and found the compliance data sufficiently reliable for our purposes. We also evaluated TSA's efforts to oversee and enforce the incident reporting requirement against criteria in *Standards for Internal Control in the Federal Government*.<sup>5</sup>

To assess the extent to which TSA has analyzed rail security incident information, we interviewed TSA officials from the TSOC, the Office of Intelligence and Analysis, the Office of Security Operations, and the Office of Security Policy and Industry Engagement regarding their roles and responsibilities. We reviewed available documentation and analyses that TSA prepared containing rail security incident information. We also examined the WebEOC incident management database to identify any limitations in the database that could present challenges for analyzing the rail security incident data, and we discussed these limitations with

---

<sup>4</sup>All TSA inspection activities must be documented and entered into PARIS, along with any findings and actions taken. We chose January 2011 as the starting point for our analysis because it was 2 full years after the regulation became effective, which would allow rail agencies and TSA a period of adjustment. June 2012 was the end of our data collection period.

<sup>5</sup>GAO, *Standards for Internal Control in the Federal Government*, [GAO/AIMD-00-21.3.1](#) (Washington, D.C.: Nov. 1, 1999).

relevant TSA officials. We also interviewed officials from the rail agencies noted earlier about their views on the information and analyses they receive from TSA on rail security incidents.

We also obtained information on how selected rail agencies applied lessons learned from foreign rail attacks to enhance their rail security measures and how rail agencies obtain and share passenger rail security-related information, including information on lessons learned from foreign rail attacks. To do this, we reviewed TSA documentation describing TSA's security strategy for the mass transit and passenger rail systems, such as TSA's Mass Transit and Passenger Rail Annex, and we discussed the rail security actions outlined in the annex with TSA officials. In addition, we reviewed rail security reports and interviewed an official from the Mineta Transportation Institute (MTI). We met with MTI because the organization's database on attacks against surface transportation, including passenger rail, was cited by TSA as the most comprehensive and up-to-date of existing databases. On the basis of information we obtained from MTI, and discussions with MTI and TSA officials, we found the quality of the methods used to develop these reports sufficient for use as a source in this report. We also interviewed security officials from selected passenger rail systems regarding their key security measures.<sup>6</sup> During visits to passenger rail systems, we toured stations and other facilities such as control centers, and observed security practices. We also interviewed officials from other federal agencies including the Central Intelligence Agency and the Department of Transportation's Federal Transit Administration and Federal Railroad Administration regarding their roles in passenger rail security, and we interviewed government officials involved with securing passenger rail in the United Kingdom. We also reviewed our prior reports on passenger rail security and information sharing as well as studies and reports conducted by outside organizations related to passenger rail, such as the Department of Homeland Security Office of the Inspector General.

---

<sup>6</sup>For some of the rail systems in our review, security is provided by the local police department. In those cases, we interviewed officials from the cognizant police department as well as security officials from the rail systems themselves.

---

# Appendix IV: Summary of Recent Attacks against Foreign Passenger Rail Systems

---

According to the Mineta Transportation Institute (MTI), from September 12, 2001 through December 31, 2011, 838 attacks occurred worldwide against passenger and commuter rail systems, resulting in 1,372 fatalities.<sup>1</sup> Most of these attacks occurred in South Asia (Pakistan, India, and Thailand) and Russia. For purposes of our review, we focused on recent passenger rail attacks that occurred in the following locations: Madrid, Spain; London, England; Mumbai, India; and Moscow, Russia. In this section, we summarize the basic facts of these attacks, using reports and information from the Department of Homeland Security (DHS), the Transportation Security Administration (TSA), open source, MTI, and others. Other attacks may have occurred at these locations, both before and after those cited.

## Madrid, Spain: March 2004

On March 11, 2004, 10 bombs exploded on three trains on Madrid's commuter rail system during the morning rush hour, killing 191 people and wounding more than 1,500 others. The bombs were placed in backpacks and detonated by cell phones. According to DHS's report on the attack, those responsible were from a terrorist group associated with al-Qaeda. According to DHS, by the end of March 2004, authorities had arrested 22 people in connection with the attack. The following month, Madrid law enforcement located a safe house associated with the suspected bombers. As authorities entered the apartment, the suspected terrorists inside detonated explosives, killing themselves and a police officer. Officers subsequently found backpacks filled with explosives and detonators in the wreckage.

---

<sup>1</sup>The MTI database—Terrorist and Serious Criminal Attacks Against Public Surface Transportation—includes data on attacks against rail and other types of surface transportation. The Mineta International Institute for Surface Transportation Policy Studies was established by the Intermodal Surface Transportation Efficiency Act of 1991. Pub. L. No. 102-240, § 6024, 105 Stat. 1914, 2188 (1991). The institute's transportation policy work is centered on, among other things, research into transportation security, planning, and policy development. According to TSA officials, this database is among the most complete and comprehensive source for surface transportation terrorist attacks. Funding for the database, about \$64,000 annually, had been provided by DHS's Science and Technology Directorate, but ceased in June 2012, as part of a broader budget reduction. The last update of the database occurred in December 2011, according to MTI. According to TSA, the agency is currently working with MTI to develop a statement of work and a contract for continued population of data to the MTI database. According to TSA, this contract will also allow TSA analysts unlimited access to the database.

London, England: July 2005

On July 7, 2005, four suicide bombers detonated improvised explosive devices during the London rush hour on three Underground (subway) trains and on a double-decker bus, killing a total of 52 people and injuring about 700. All four bombers were also killed in the attacks. The three Underground attacks occurred within moments of one another and the bus bombing occurred approximately 1 hour later. The bombers traveled together from a commuter rail station north of London to the King's Cross Underground station, from which they departed to their respective attack destinations. A second series of attacks was attempted 2 weeks later, on July 21. However, the explosives failed to detonate. According to DHS, no terrorist group has claimed responsibility. After a police investigation of the attacks, three additional suspects were charged with conspiracy in the identification and reconnaissance of potential terrorist targets in London. However, all three were acquitted on those charges in April 2009.

Mumbai, India: July 2006 and  
November 2008

On July 11, 2006, a series of seven explosions occurred on a single rail line of Mumbai's commuter railway. In all, 190 people were killed and 625 were injured across all the incidents. In September 2006, Indian police said that the attacks were executed by Lashkar-e-Taiba.

Starting on November 26, 2008, and continuing for the next 2 days, terrorists attacked various locations in the Mumbai area including a passenger rail station and hotels catering to Western tourists. The attackers used assault weapons, small arms, grenades, and explosives. One of the first attacks occurred at the Chhatrapati Shivaji rail terminus, one of the busiest train stations in the country. Two gunmen entered the passenger hall and opened fire, killing 59 and injuring 104. The terrorists then dispersed throughout the city attacking another eight locations, killing at least an additional 129 and injuring more than 223 others. According to DHS, like the attacks on July 11, 2006, the terrorists were also from Lashkar-e-Taiba. Nine terrorists were killed during the course of the attacks, while one was captured alive.

Moscow, Russia: March 2010

On March 29, 2010, two suicide bombers attacked trains at two stations in the Moscow Metro during the morning rush hour, killing 40 and injuring 58 others. The first explosion occurred on a train as it pulled into Lubyanka station. The second explosion occurred at the Park Kultury station as passengers were boarding a train. Both the Lubyanka and Park Kultury stations are transfer stations and may have been chosen by the attackers in an effort to target the greatest number of people. Russian officials attribute the attack to Chechen separatists.



# Appendix V: Comments from the Department of Homeland Security

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



**Homeland  
Security**

December 4, 2012

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

Re: GAO Draft Report 13-20, PASSENGER RAIL SECURITY: Consistent Incident Reporting and Analysis Needed to Achieve Program Objectives

Dear Mr. Lord:

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

As highlighted in the report, the Transportation Security Administration (TSA) has both a vital and primary federal role in passenger rail security, and its success in this domain is pivotal to national security. While GAO notes that there have been no terrorist attacks against U.S. passenger rail systems, passenger rail security has vulnerabilities that adversaries may attempt to exploit. This has been made evident by several alleged terrorist plots uncovered in the United States and overseas in the last several years.

This current threat has produced several proactive steps on the part of TSA to protect the nearly 15 million daily riders of mass transit and passenger rail systems nationwide. These actions include, among other initiatives, implementation of regulations that are the subject of this review, as well as TSA's incorporation of a comprehensive, strategic, and risk-based approach to rail security.

In response to GAO's findings, TSA is taking active steps to strengthen the passenger rail security reporting and analysis continuum through upgrades to guidance protocols and data collection methodology. On the front end of the process, TSA agrees with GAO that clarifying written guidance directed at both TSA inspectors and rail agencies is the right course of action. Additionally, the Transportation Security Operations Center (TSOC) has already implemented protocols to ensure that data entry is consistent and complete. The need for uniform, accurate, and complete reporting of passenger rail data is paramount.

Significantly, in support of GAO's recommendation for greater oversight of local inspection activities, the TSA Office of Security Operations (OSO) Compliance Programs has granted Regional Security Inspectors (RSIs) with review privileges to provide greater visibility on all surface inspections entered into the Performance and Results Information System (PARIS).

Taken together, these efforts should produce greater dividends related to continuous trend analysis and ultimately, implementation of security measures that detect and deter terrorism.

Finally, TSA continues to maintain collaborative working relationships with industry representatives within mass transit and passenger rail agencies; which will enhance rail security and improve communication with respect to incident reporting.

The GAO's draft report contained five recommendations with which DHS concurs. Specifically, GAO recommended the Administrator of the Transportation Security Administration:

**Recommendation 1:** Develop and disseminate written guidance for local TSA inspection officials and rail agencies that clarifies the types of incidents that should be reported to the TSOC.

**Response:** Concur. TSA OSO and the Office of Security Policy and Industry Engagement (OSPIE) will work together to develop written guidance for passenger rail agencies clarifying the types of incidents that should be reported to the TSOC. TSA will then disseminate the guidance to these passenger rail agencies.

**Recommendation 2:** Enhance and utilize existing oversight mechanisms at the Headquarters level, as intended, to provide additional management oversight of local compliance inspections and enforcement actions.

**Response:** Concur. TSA has several mechanisms in place at the Headquarters (HQ) level to manage and oversee compliance and enforcement actions in the field. Within the TSA OSO Office of Compliance Programs, Surface Compliance Branch, RSIs serve as the principal technical specialists at the national level for compliance oversight activities for surface transportation. RSIs oversee and implement transportation security measures, policy, programs, and operations. RSIs conduct field office audits as well as field office visits as a mechanism to provide HQ oversight of local compliance inspections and enforcement actions for consistency and continuity. TSA HQ conducts monthly calls and holds quarterly visits with RSIs.

Additionally, while the TSA OSO Office of Compliance Programs manages and oversees inspections, investigations, and recommendations for enforcement action, TSA's Office of Chief Counsel (OCC) within HQ manages and oversees TSA's enforcement actions. Field inspection offices coordinate enforcement actions with local field counsel. Local field counsels coordinate these enforcement actions with the TSA OCC Enforcement Division. In addition to coordinating enforcement actions with RSIs and the local field offices, the TSA OCC coordinates enforcement actions with OSO Office of Compliance Programs and with OSPIE.

While TSA believes that several mechanisms and layers are in place for the oversight and management of local inspection and enforcement actions, TSA recognizes that there are always opportunities for improving oversight. In order to improve HQ oversight and management of local compliance inspections and enforcement actions, RSIs recently have been granted case review privileges in PARIS. This will allow the Surface RSIs even greater visibility on all Surface inspections, investigations, and recommendations for enforcement actions entered into

PARIS by enabling them to provide written recommendations in PARIS prior to inspection approval. This effort will memorialize RSI guidance and provide greater quality control of cases.

**Recommendation 3:** Establish a process for updating the database when incidents that had not previously been reported are discovered through compliance activities.

**Response:** Concur. TSA, through the TSOC and the OSO Office of Compliance Programs, is currently establishing a business process to ensure the relevant databases are complete. Once this process is finalized, the TSOC will update the WebEOC (Emergency Operations Center) to allow Compliance/Inspectors to input records into the system to denote reports that are not reported to the TSOC and discovered via compliance activities.

**Recommendation 4:** Develop guidance for TSOC officials that includes definitions of data entry options to reduce errors resulting from data entry problems.


**Response:** Concur. TSA, through the TSOC, completed this recommendation at close of the exit conference by updating the guidance for TSOC Watch Officer with respect to WebEOC input options.

**Recommendation 5:** Establish a systematic process for regularly conducting trend analysis of the rail security incident data, in an effort to identify potential security trends that could help the agency anticipate or prevent an attack against passenger rail and develop recommended security measures.

**Response:** Concur. The TSA Office of Intelligence and Analysis will work with OSPIE to develop a process to review suspicious activities and incidents in the mass transit and passenger rail arenas in order to identify trends which might represent a threat to transportation.

Again, thank you for the opportunity to review and comment on this draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Sincerely,

  
For Jim H. Crumpacker  
Director  
Departmental GAO-OIG Liaison Office

---

# Appendix VI: GAO Contact and Staff Acknowledgments

---

## GAO Contact

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

---

## Staff Acknowledgments

In addition to the contact named above, Jessica Lucas-Judy (Assistant Director), Eric Hauswirth, Adam Hoffman, Tracey King, Elizabeth Kowalewski, Kelly Rubin, and Jonathan Tumin made key contributions to this report.

---

## GAO's Mission

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

---

## Obtaining Copies of GAO Reports and Testimony

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

---

## Order by Phone

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

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

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

---

## Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#).  
Subscribe to our [RSS Feeds](#) or [E-mail Updates](#). Listen to our [Podcasts](#).  
Visit GAO on the web at [www.gao.gov](http://www.gao.gov).

---

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <http://www.gao.gov/fraudnet/fraudnet.htm>

E-mail: [fraudnet@gao.gov](mailto:fraudnet@gao.gov)

Automated answering system: (800) 424-5454 or (202) 512-7470

---

## Congressional Relations

Katherine Siggerud, Managing Director, [siggerudk@gao.gov](mailto:siggerudk@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](mailto:youngc1@gao.gov), (202) 512-4800  
U.S. Government Accountability Office, 441 G Street NW, Room 7149  
Washington, DC 20548

