United States Government Accountability Office

Testimony Before the Subcommittees on Transportation Security and Counterterrorism and Intelligence, Committee on Homeland Security, House of Representatives

For Release on Delivery
Expected at 2:00 p.m. ET
Thursday, September 17, 2015

SURFACE TRANSPORTATION SECURITY

TSA Has Taken Steps Designed to Develop Processes for Sharing and Analyzing Information and to Improve Rail Security Incident Reporting

Statement of Jennifer Grover, Director, Homeland Security and Justice

Accessible Version

September 2015

SURFACE TRANSPORTATION SECURITY

TSA Has Taken Steps Designed to Develop Processes for Sharing and Analyzing Information and to Improve Rail Security Incident Reporting

GAO Highlights

Highlights of GAO-15-205T, a testimony before the Subcommittees on Transportation Security and Counterterrorism and Intelligence, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

The U.S. surface transportation system's size and importance to the country's safety, security, and economic well-being make it an attractive target for terrorists. Within the federal government, TSA–a component of the Department of Homeland Security–is the primary federal agency responsible for overseeing and enhancing the security of the surface transportation system. A key component of this responsibility is ensuring that security-related information is collected, analyzed, and shared effectively across all modes, including rail. 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.

This testimony addresses the extent to which TSA has (1) developed systematic processes for integrating stakeholder feedback about security-related information it provides and analyzing trends in reported rail security incidents and (2) ensured consistent implementation of rail security incident reporting requirements. This statement is based on related GAO reports issued in June 2014 and December 2012, including selected updates on TSA's efforts to implement GAO's prior recommendations related to rail security and information sharing. For the selected updates, GAO reviewed related documentation, including tools TSA developed to provide oversight. GAO also interviewed TSA officials.

What GAO Recommends

GAO is making no new recommendations in this statement.

View GAO-15-205T. For more information, contact Jennifer Grover, (202) 512-7141, or GroverJ@gao.gov.

What GAO Found

In June 2014, GAO found that the Transportation Security Administration (TSA) did not have a systematic process for incorporating stakeholder feedback to improve security-related information sharing and recommended that TSA systematically document and incorporate stakeholder feedback. TSA concurred with this recommendation and, in April 2015, TSA developed a standard operating procedure to help ensure proper evaluation and consideration of all feedback TSA receives. In December 2012, GAO found TSA had made limited use of the rail security incident information it had collected from rail agencies, in part because it did not have a systematic process for conducting trend analysis. TSA's purpose for collecting this information was to allow TSA to "connect the dots" through trend analysis. However, the incident information provided to rail agencies by TSA was generally limited to descriptions of specific incidents. As a result, officials from passenger rail agencies GAO spoke with reported that they generally found little value in TSA's incident reporting requirement. On the basis of these findings, GAO recommended that TSA establish a systematic process for regularly conducting trend analysis of the rail security incident data. Although GAO has not assessed the effectiveness of TSA's efforts, by August 2013, TSA had developed a new analysis capability that, among other things, produces Trend Analysis Reports from the incident data.

In December 2012, GAO found that TSA had not provided consistent oversight of its rail security reporting requirement, which led to variation in the types and number of passenger rail security incidents reported. Specifically, GAO found that TSA headquarters had not provided guidance to local TSA inspection officials, the primary TSA points of contact for rail agencies, about the types of rail security incidents that must be reported, which contributed to inconsistent interpretation of the regulation. The variation in reporting was compounded by inconsistencies in compliance inspections and enforcement actions, in part because of limited utilization of oversight mechanisms at the headquarters level. GAO also found that TSA's incident management data system, WebEOC, had incomplete information, was prone to data entry errors, and had other limitations that inhibited TSA's ability to search and extract basic information. On the basis of these findings, GAO recommended that TSA (1) develop and disseminate written guidance on the types of incidents that should be reported, (2) enhance existing oversight mechanisms for compliance inspections and enforcement actions, (3) establish a process for updating WebEOC with previously unreported incidents, and (4) develop guidance to reduce data entry errors. TSA concurred with these recommendations and has taken actions to implement them. Specifically, in September 2013, TSA disseminated written guidance to local TSA inspection officials and passenger and freight rail agencies that provides clarification about the rail security incident reporting requirement. In August 2013, TSA enhanced existing oversight mechanisms by creating an inspection review mechanism, among other things. TSA also established a process for updating WebEOC in March 2013, and in October 2014, officials reported that they have updated the guidance used by officials responsible for entering incident data to reduce data entry errors associated with incident types. Although GAO has not assessed the effectiveness of these efforts, they address the intent of the recommendations.

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

Chairmen Katko and King, Ranking Members Rice and Higgins, and Members of the Subcommittees:

I appreciate the opportunity to participate in today's hearing to discuss our work related to the Transportation Security Administration's (TSA) efforts to secure the U.S. surface transportation system, particularly those associated with passenger and freight rail.[1] The transportation system's size and importance to the country's safety, security, and economic well-being make it an attractive target for terrorists. As shown by the active shooter incident that occurred on a train traveling from Amsterdam to Paris on August 21, 2015, rail systems are inherently 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, lack of barriers to access. One of the critical challenges facing rail system operators—and the federal agencies that regulate and oversee them—is finding ways to protect rail systems from potential terrorist attacks without compromising the accessibility and efficiency of rail travel.

Within the federal government, TSA—a component of the Department of Homeland Security (DHS)—is the primary federal agency responsible for security in all modes of transportation, including aviation, passenger and freight rail, highway and motor carrier, maritime, and pipeline.[2] A key component of this responsibility is ensuring that information related to transportation security and potential threats across all modes is collected, analyzed, and shared effectively. Disrupted terrorist attacks in recent years, such as the April 2013 disruption of a planned attack on a passenger train operating between Toronto and New York City, highlight the importance of reporting and sharing security-related information. TSA's other responsibilities, however, vary by transportation mode. Specifically, TSA has a direct role in ensuring the security of the aviation mode through its management of a passenger and baggage screener

[1]The surface transportation modes include passenger rail (such as subway-type mass transit systems and intercity rail such as Amtrak), freight rail, highway and commercial vehicle, and pipeline.

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

workforce that inspects individuals and their property to deter and prevent an act of violence or air piracy. In contrast, TSA's responsibilities for securing surface transportation systems such as passenger and freight rail systems have primarily included developing national strategies, establishing security standards, and conducting assessments and inspections of surface transportation modes, while public and private sector transportation operators are responsible for implementing security measures for their systems. TSA's annual budget further highlights the difference between TSA's roles in securing the aviation and surface transportation modes. For example, the DHS Appropriations Act, 2015, enacted March 4, 2015, appropriated $123,749,000 for surface transportation security compared with $5,639,095,000 for aviation security.[3]

My statement today addresses the extent to which TSA has (1) developed systematic processes for integrating stakeholder feedback about security-related information provided by the agency and analyzing trends in reported rail security incidents and (2) ensured consistent implementation of rail security incident reporting requirements. This statement is based on related GAO reports issued in December 2012 and June 2014, including selected updates on TSA's efforts to implement our prior recommendations related to information sharing and rail security.[4] To conduct our earlier work, among other things, we conducted a survey of 481 transportation stakeholders, including freight and passenger rail stakeholders, from November 2013 through January 2014, regarding their satisfaction with TSA's sharing of security-related information. We received responses from 337 stakeholders (a 70 percent response rate). We also reviewed TSA policy documents and guidance on rail security reporting requirements, and passenger rail security incident data from

[3]Pub. L. No. 114-4, 129 Stat. 39, 44-46 (2015). The approximately $124 million and $5.6 billion appropriated to TSA's Surface Transportation Security and Aviation Security accounts, respectively, do not reflect amounts appropriated to TSA's Intelligence and Vetting and Transportation Security Support accounts, which also support TSA's surface and aviation security missions, as well as the $250 million in fee collections available to TSA through the Aviation Security Capital Fund to support security-related airport improvement projects and the procurement and installation of explosives detection systems for use at airports.

[4]GAO, *Transportation Security Information Sharing: Stakeholder Satisfaction Varies; TSA Could Take Additional Actions to Strengthen Efforts*. GAO-14-506 (Washington, D.C.: June 24, 2014), and *Passenger Rail Security: Consistent Incident Reporting and Analysis Needed to Achieve Program Objectives*. GAO-13-20 (Washington, D.C.: Dec. 19, 2012).

January 2011 through June 2012. The reports cited in this statement provide detailed information about our scope and methodology. For the selected updates, we reviewed related documentation and interviewed TSA officials on TSA's progress in addressing our recommendations. This documentation includes tools TSA developed to provide oversight of the rail security incident reporting process, guidance for TSA inspectors and rail agencies, and updates to TSA's data management system, among other things. The work upon which this statement is based was conducted 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

The Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act) directed DHS to create a plan for sharing transportation security–related information among public and private entities that have a stake in protecting the nation's transportation system, including passenger and freight rail. This plan—first issued in July 2008—is now called the Transportation Security Information Sharing Environment (TSISE).[5] The TSISE describes, among other things, the information–sharing process. TSA disseminates security information through several information products, including reports, assessments, and briefings, among others. These products are distributed through mechanisms including the Homeland Security Information Network and mechanisms sponsored by industry, such as the Association of American Railroads' Railway Alert Network, among others.

TSA is also specifically responsible for receiving, assessing, and distributing intelligence information related to potential threats and significant security concerns (rail security incidents) related to the nation's rail system. Specifically, in 2008, TSA issued a regulation requiring U.S. rail systems to report all rail security incidents to TSA's Transportation

[5]Pub. L. No. 110-53, § 1203(a), 121 Stat. 266, 383-85 (2007) (codified at 49 U.S.C. § 114(u)). The TSISE was formerly called the Transportation Security Information Sharing Plan (TSISP). In fiscal year 2013, TSA renamed the plan the TSISE to reflect that the TSISE is not a part of a plan, but rather a series of processes.

Security Operations Center (TSOC), among other things.[6] The TSOC is an operations center open 24 hours a day, 7 days a week, that serves as TSA's main point of contact for monitoring security–related incidents or crises in all modes of transportation. The regulation also authorizes TSA officials to view, inspect, and copy rail agencies' records as necessary to enforce the rail security incident reporting requirements.[7] This regulation 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. TSA's regulation is intended to provide the agency with essential information on rail security incidents so that TSA can conduct comprehensive intelligence analysis, threat assessment, and allocation of security resources, among other things.[8] According to the regulation, potential threats and significant security concerns that must be reported to the TSOC include bomb threats, suspicious items, or indications of tampering with rail cars, among others.[9]

Within TSA, different offices are responsible for sharing transportation security–related information and for implementing and enforcing the rail security incident reporting requirement. For instance, TSA's Office of Security Policy and Industry Engagement (OSPIE) is the primary point of contact for sharing information with private sector stakeholders, and is responsible for using incident reports and analyses, among other things, to develop strategies, policies, and programs for rail security, including

[6]49 C.F.R. §§ 1580.105, .203. These requirements generally apply to passenger and freight rail carriers, as well as rail hazardous materials shippers and rail hazardous materials receivers located within high-threat urban areas. The regulation also requires rail agencies to designate rail security coordinators, and codifies TSA's authority to conduct security inspections of rail agency property. 49 C.F.R. §§ 1580.101, .201.5 This is the only rule that TSA has issued to date regarding passenger rail security. Additional rules have been issued regarding freight rail security, specifically requirements related to rail shipments of specified hazardous materials. The Implementing Recommendations of the 9/11 Commission Act of 2007 also 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, 409-11 (codified at 49 U.S.C. § 1137). As of September 2015, a draft regulation had not been submitted for public comment. According to TSA, the training rule is among the agency's highest priorities, but officials did not provide a target date for when the revised regulation will be provided for public comment.

[7]49 C.F.R. § 1580.5.

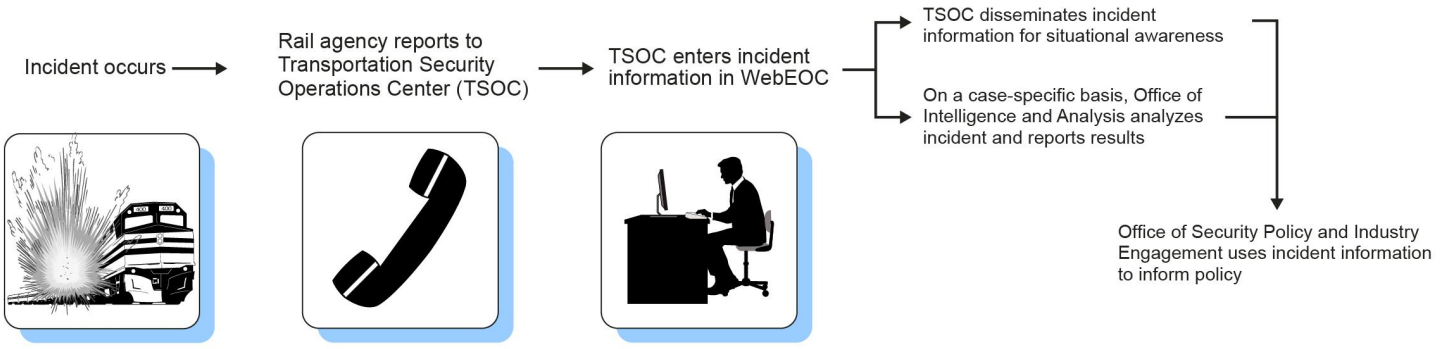
[8]71 Fed. Reg. 76,852, 76,876 (Dec. 21, 2006).

[9]49 C.F.R. § 1580.105(c), .203(c).

operational security activities, training exercises, public awareness, and technology. TSA's Office of Intelligence and Analysis (OIA) receives intelligence information regarding threats to transportation and designs intelligence products intended for officials in TSA, other parts of the federal government, state and local officials, and industry officials, including rail agency security coordinators and law enforcement officials.

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 selected TSA officials; other federal, state, and local government officials; and selected rail agencies' law enforcement officials. Figure 1 shows the intended steps and responsibilities of TSA components involved in the rail security incident reporting process.

Figure 1: The Intended Rail Security Reporting Process



Source: GAO analysis of TSA information; Art Explosion (graphics). | GAO-15-205T

Accessible Text for Figure 1: The Intended Rail Security Reporting Process

1) Incident occurs;

2) Rail agency reports to Transportation Security Operations Center (TSOC);

3) TSOC enters incident information in WebEOC;

4)

a) TSOC disseminates incident information for situational awareness;

b) On a case-specific basis, Office of Intelligence and Analysis analyzes incident and reports results;

5) Office of Security Policy and Industry Engagement uses incident information to inform policy.

Source: GAO analysis of TSA information; Art Explosion (graphics). | GAO-15-205T

TSA's Office of Security Operations (OSO) 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 270 transportation security inspectors–surface (TSI-S) nationwide.[10] The TSI-Ss are responsible for, among other things, providing clarification to rail agencies regarding the incident reporting process and for overseeing rail agencies' compliance with the reporting requirement by conducting inspections to ensure that incidents were properly reported to the TSOC. 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.

[10]There are currently 49 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, as of September 2015, TSA has deployed 496 air cargo inspectors and 672 aviation regulation inspectors.

TSA Has Developed Processes Designed to Integrate Stakeholder Feedback and Address Gaps in Trend Analysis

TSA Has Developed a Process Designed to Incorporate Feedback on Security-Related Information

In June 2014, we found that TSA had some mechanisms in place to collect stakeholder feedback on the products it disseminates containing security-related information and had initiated efforts to improve how it obtains customer feedback, but had not developed a systematic process for collecting and integrating such feedback.[11] Specifically, in February 2014, TSA reconvened its Information Sharing Integrated Project Team (IPT), whose charter included, among other things, milestones and time frames for developing a centralized management framework to capture stakeholder satisfaction survey data on all of TSA's security-related products and the systems used to distribute these products.[12] However, at the time of our June 2014 report, the IPT Charter did not specify how TSA planned to systematically collect, document, and incorporate informal feedback—a key mechanism used by the majority of the stakeholders we surveyed, and a mechanism TSA officials told us they utilize to improve information sharing. For instance, the rail industry provided TSA with a list of areas for emphasis in intelligence analysis in December 2012, and TSA subsequently initiated a product line focusing on indications and warnings associated with disrupted or successful terrorist attacks. TSA officials stated that they further refined one of the products as a result of a stakeholder requesting information on tactics used in foreign rail attacks.

[11]GAO-14-506. Mechanisms include surveys attached to security-related information products and informal feedback collected at meetings with stakeholders.

[12]According to TSA officials, TSA formed the IPT in 2009 but planning stopped because of multiple TSA organization realignments. IPT members include OIA, OSPIE, and other TSA components, as well as external entities, such as the DHS Office of Intelligence and Analysis, stakeholders, and trade associations. One of the primary missions of the IPT is to evaluate TSA's information-sharing services across all modes of transportation.

In 2013, one TSA component built a system to track informal information sharing with stakeholders at meetings and conferences, and through e-mail, but TSA officials stated that the data were not used for operational purposes, and TSA had no plans to incorporate this system into its centralized management framework because the IPT had decided to focus its initial efforts on developing a survey mechanism.

According to our June 2014 survey results, surface transportation stakeholders were generally satisfied with TSA's security-related products and the mechanisms used to disseminate them.[13] In particular, 63 percent of rail stakeholders (70 of 111) reported that they were satisfied with the products they received in 2013, and 54 percent (59 of 110) reported that they were satisfied with security-related information sharing mechanisms.[14] However, because TSA lacked specific plans and documentation related to improving its efforts to incorporate all of its stakeholder feedback, it was unclear how, or if, TSA planned to use stakeholder feedback to improve information sharing. As a result of these findings, we recommended that TSA include in its planned customer feedback framework a systematic process to document informal feedback, and how it incorporates all of the feedback TSA receives, both formal and informal. TSA concurred, and in response, by April 2015, had taken actions to develop these processes. Specifically, TSA developed a

[13]Sixty-seven percent of surface transportation stakeholders (125 of 186) reported that they were satisfied with the security-related products they received from TSA in 2013, and 58 percent of surface transportation stakeholders (106 of 183) reported that they were satisfied with the mechanisms used to disseminate this information. Respondents who were not satisfied with TSA's security-related products or information-sharing mechanisms cited concerns that the information provided was often dated, among other issues. Survey respondents were asked to rate their organization's satisfaction using the following terms: "very satisfied," "somewhat satisfied," "neither satisfied nor dissatisfied," "somewhat dissatisfied," "very dissatisfied," and "don't know." We use the term "satisfied" to describe organizations that indicated they were either "very satisfied" or "somewhat satisfied." Similarly, we use the term "dissatisfied" to describe organizations that indicated they were either "very dissatisfied" or "somewhat dissatisfied" with the information they received. Because satisfaction and dissatisfaction were not the only possible responses, when we report that 59 percent of respondents reported being satisfied, for example, that does not necessarily mean that 41 percent were dissatisfied.

[14]These results for rail stakeholders differ from those reported in GAO-14-506 because they represent the survey responses we received from all passenger and freight rail agencies. The "public transit" category in GAO-14-506 included 13 agencies in modes other than rail. To arrive at the numbers in this statement, we combined the responses of the 23 rail agencies in the public transit category with the responses received from 88 and 87 rail agencies in response to our questions on satisfaction with TSA products and mechanisms, respectively.

standard operating procedure to organize how its offices solicit, receive, respond to, and document both formal and informal customer feedback on its information-sharing efforts, which delineates a systematic process for doing so. TSA also developed a TSA-wide standard survey for its offices to use to obtain formal and informal feedback on specific products, and created an information-sharing e-mail inbox to which all survey responses will be sent, evaluated, and distributed to the appropriate office for action. We have not evaluated these actions, but if implemented effectively, we believe that TSA will now be better positioned to meet stakeholder needs for security-related information.

TSA Efforts Should Help Address Gaps in Conducting Trend Analysis of Rail Security Incident Information

In December 2012, we found TSA had made limited use of the rail security incident information it had collected from rail agencies, in part because it did not have a systematic process for conducting trend analysis.[15] TSA's stated purpose for collecting rail security incident information was to allow TSA to "connect the dots" by conducting trend analysis that could help TSA and rail agencies develop targeted security measures. However, the incident information provided to rail agencies by TSA was generally limited to descriptions of specific incidents with minimal accompanying analysis. As a result, officials from passenger rail agencies we spoke with generally found little value in TSA's incident 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 rail agencies develop appropriate security measures. However, as we reported in December 2012, opportunities for more sophisticated trend analysis existed. For example, the freight 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, the Railway Alert Network subsequently issued guidance to its member organizations designed to increase awareness of this trend 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 and was contained in TSA's incident management system, WebEOC.

[15]GAO-13-20.

On the basis of these findings, in December 2012, we recommended 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 that could help the agency anticipate or prevent an attack against passenger rail and develop recommended security measures. TSA concurred with this recommendation and by August 2013 had developed a new capability for identifying trends in the rail security incident data, known as the Surface Compliance Trend Analysis Network (SCAN). SCAN is designed to identify linkages between incidents captured in various sources of data, assemble detailed information about these incidents, and accurately analyze the data to enhance the agency's ability to detect impending threats. According to TSA officials, SCAN consists of three elements: two OSO surface detailees located at TSOC, enhanced IT capabilities, and a new rail security incident analysis product for stakeholders. According to TSA, one of the key functions of the surface detailees is to continuously look for trends and patterns in the rail security incident data that are reported to TSOC, and to coordinate with OSPIE and OIA to conduct further investigations into potential trends. As I will discuss later in this statement, TSA has also made improvements to WebEOC, including steps to improve the completeness and accuracy of the data and the ability to produce basic summary reports, which we believe should facilitate this type of continuous trend analysis.

TSA generates a Trend Analysis Report for any potential security trends the surface detailees identify from the rail security incident data. The Trend Analysis Report integrates incident information from WebEOC with information from multiple other sources, including TSA's compliance database and media reports, and provides rail agencies and other stakeholders with analysis of possible security issues that could affect operations as a result of these trends. According to TSA officials, since SCAN was established, approximately 13 Trend Analysis Reports have been produced and disseminated to local TSA inspection officials and rail agencies. Although we have not assessed the effectiveness of these efforts to better utilize rail security information, we believe these actions address the intent of our recommendation. Further, if implemented effectively, they should better position TSA to provide valuable analysis on rail security incidents and to develop recommended security measures for rail agencies, as appropriate.

TSA Has Taken Steps to Improve Consistent Implementation of the Rail Security Incident Reporting Process

TSA Has Taken Steps to Improve the Consistency of the Rail Security Incident Reporting Process

In December 2012, we found that TSA had not provided consistent oversight of the implementation of the rail security reporting requirement, which led to considerable variation in the types and number of passenger rail security incidents reported.[16] Specifically, we found that TSA headquarters had not provided guidance to local TSA inspection officials, the primary TSA points of contact for rail agencies, about the types of rail security incidents that must be reported, a fact that contributed to inconsistent interpretation of the regulation by local TSA inspection officials.[17] While some variation was expected in the number of rail security incidents that rail agencies reported because of differences in agency size, geographic location, and ridership, passenger rail agencies we spoke with at the time reported receiving inconsistent feedback from their local TSA officials regarding certain types of incidents, such as those involving weapons. As a result, we found that, for 7 of the 19 passenger rail agencies included in our review, the number of incidents reported per million riders ranged from 0.25 to 23.15.[18]

[16]GAO-13-20

[17]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. “Local TSA inspection officials” refers to TSI-Ss and AFSD-Is.

[18]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 statement. Because of limitations associated with identifying the total number of incidents by agency, we limited this analysis to 7 of the 19 passenger rail agencies that we included in our review. Ridership data for 2011 were provided by the American Public Transportation Association.

This variation we identified was compounded by inconsistencies in compliance inspections and enforcement actions, in part because of limited utilization of oversight mechanisms at the headquarters level. For example, in December 2012, we found that TSA established the RSI-S position as a primary oversight mechanism at the headquarters level for monitoring rail security compliance inspections and enforcement actions to help ensure consistency across field offices. However, at the time of our report, the RSI-S was not part of the formal inspection process and had no authority to ensure that inspections were conducted consistently. We also found that the RSI-S had limited visibility over when and where inspections were completed or enforcement actions were taken because TSA lacked a process to systematically provide the RSI-S with this information during the course of normal operations. As a result, our analysis of inspection data from January 1, 2011, through June 30, 2012, showed that average monthly inspections for the 19 rail agencies in our review ranged from about eight inspections to no inspections, and there was variation in the regularity with which inspections occurred.[19] We also found that TSA inconsistently applied enforcement actions against passenger rail agencies for not complying with the reporting requirement. For example, 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, despite having been inspected.

On the basis of these findings, in December 2012, we recommended that TSA: (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 and (2) enhance and utilize existing oversight mechanisms at the headquarters level, as intended, to provide management oversight of local compliance inspections and enforcement actions. TSA concurred with both of these recommendations and has taken actions to implement them. Specifically, in September 2013, TSA disseminated written guidance to local TSA inspection officials and passenger and freight rail agencies that provides clarification about the requirements of the rail security incident reporting process. This guidance includes examples and descriptions of the types of incidents that should be reported under the regulatory criteria, as well as details about the type

[19]We reviewed inspection data for 19 passenger rail agencies. Three passenger rail agencies had not been inspected, including a major metropolitan rail agency. Local officials we interviewed said it was unlikely that no incidents had occurred at that agency.

of information that should be included in the incident report provided to the TSOC. Further, as of August 2013, TSA had established an RSI-dashboard report that provides weekly, monthly, and quarterly information about the number of inspection reports that have been reviewed, accepted, and rejected. According to TSA officials, this helps ensure that rail agencies are inspected regularly, by providing the RSI-Ss with greater insight into inspection activities. TSA has also enhanced the utilization of the RSI-Ss by providing them with the ability to review both passenger and freight rail inspections before the inspection reports are finalized and enforcement action is taken. According to TSA officials, this allows the RSI-Ss to ensure that enforcement actions are applied consistently by local TSA inspection officials. TSA also developed a mechanism for tracking the recommendations RSI-Ss make to local TSA inspection officials regarding changes to local compliance inspections, as well as any actions that are taken in response. Collectively, we believe that these changes should allow the RSI-Ss to provide better management oversight of passenger and freight rail regulatory inspections and enforcement actions, though we have not assessed whether they have done so. We also believe these actions, if implemented effectively, will help ensure that the rail security incident reporting process is consistently implemented and enforced, and will address the intent of our recommendations.

TSA Has Taken Steps to Improve the Accuracy and Completeness of Incident Data

In December 2012, we also found that TSA's incident management data system, known as WebEOC, had incomplete information, was prone to data entry errors, and had other limitations that inhibited TSA's ability to search and extract basic information.[20] These weaknesses in WebEOC hindered TSA's ability to use rail security incident data to identify security trends or potential threats. Specifically, at the time of our 2012 report, TSA did not have an established process for ensuring that WebEOC was updated to include information about rail security incidents that had not been properly reported to the TSOC.[21] As a result, of the 18 findings of noncompliance we reviewed that were a result of failure to report an incident, 13 were never entered into WebEOC, and consequently could not be used by TSA to identify potential security trends. In addition, in December 2012, we found that TSA's guidance for officials responsible for entering incident data was insufficient, a fact that may have

[20]GAO-13-20.

[21]TSA could become aware of such an incident through a compliance inspection, media reports, or other governmental incident management systems.

contributed to data entry errors in key fields, including the incident type and the mode of transportation (such as mass transit or freight rail). At the time of our report, because of data errors and technical limitations in WebEOC, TSA also could not provide us with basic summary information about the rail security incident data contained in WebEOC, such as the number of incidents reported by incident type (e.g., suspicious item or bomb threat), by a particular rail agency, or the total number of rail security incidents that have been reported to the TSOC.[22] Without the ability to identify this information on the number of incidents by type or the total number of incidents, we concluded that TSA faced challenges determining if patterns or trends exist in the data, as the reporting system was intended to do.

On the basis of these findings, in December 2012 we recommended that TSA (1) establish a process for updating WebEOC when incidents that had not previously been reported are discovered through compliance activities, and (2) develop guidance for TSOC officials that includes definitions of data entry options to reduce errors resulting from data entry problems. TSA concurred with both of these recommendations and has taken actions to implement them. Specifically, in March 2013, TSA established a process for the surface detailee position, discussed earlier in this statement, to update WebEOC when previously unreported incidents are discovered through compliance activities. Additionally, in October 2014, TSA officials reported they have updated the guidance used by TSOC officials responsible for entering incident data into WebEOC to include definitions of incident types. TSA has also made changes to WebEOC that will allow for officials to search for basic information, such as the total number of certain types of incidents, required to facilitate analysis. We have not reevaluated the data contained in WebEOC, but we believe that the changes TSA has made should allow the agency to conduct continuous analysis of the rail security incident data to identify potential trends. We believe these actions address the intent of our recommendations and, if implemented effectively, should improve the accuracy and completeness of the incident data in WebEOC. This should provide TSA with a more comprehensive

[22]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 selected 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.

picture of security incidents as well as allow it to better identify any trends or patterns.

Chairmen Katko and King, Ranking Members Rice and Higgins, and members of the subcommittees this concludes my prepared statement. I would be happy to respond to any questions you may have at this time.

GAO Contact and Staff Acknowledgments

For questions about this statement, please contact Jennifer Grover at (202) 512-7141 or groverj@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Individuals making key contributions to this statement include Chris Ferencik (Assistant Director), Michele Fejfar, Paul Hobart, Adam Hoffman, Tracey King, Elizabeth Kowalewski, Brendan Kretzschmar, Kelly Rubin, and Christopher Yun. Key contributors to the previous work that this testimony is based on are listed in those reports.