



SEPTEMBER 17, 2015

SAFEGUARDING OUR NATION'S SURFACE TRANSPORTATION SYSTEMS AGAINST EVOLVING TERRORIST THREATS

U.S. HOUSE OF REPRESENTATIVES, COMMITTEE ON HOMELAND SECURITY, SUBCOMMITTEE
ON COUNTERTERRORISM AND INTELLIGENCE, AND SUBCOMMITTEE ON TRANSPORTATION
SECURITY

ONE HUNDRED FOURTEENTH CONGRESS, FIRST SESSION

HEARING CONTENTS:

MEMBER STATEMENTS

John Katko [\[view PDF\]](#)
Subcommittee Chairman
Subcommittee on Transportation Security

Peter T. King [\[view PDF\]](#)
Subcommittee Chairman
Subcommittee on Counterterrorism and Intelligence

WITNESS TESTIMONY

Eddie Mayenschein [\[view PDF\]](#)
Assistant Administrator
Office of Security Policy and Industry Engagement
Transportation Security Administration
U.S. Department of Homeland Security

Jennifer Grover [\[view PDF\]](#)
Director
Transportation Security and Coast Guard Issues
Homeland Security and Justice Team
U.S. Government Accountability Office

Raymond Diaz [\[view PDF\]](#)
Director of Security
Metropolitan Transportation Authority (New York)

Polly Hanson [\[view PDF\]](#)
Chief Of Police
National Railroad Passenger Corporation (Amtrak)

AVAILABLE WEBCAST(S):*

Full Hearing: <https://youtu.be/2pYJRMKfQbc>

COMPILED FROM:

- <https://homeland.house.gov/hearing/joint-subcommittee-hearing-safeguarding-nations-surface-transportation-systems-evolving-terrorist-threats/>

** Please note: Any external links included in this compilation were functional at its creation but are not maintained thereafter.*



OPENING STATEMENT

September 17, 2015

MEDIA CONTACTS

Susan Phalen, Matthew Ballard

**Statement of Subcommittee Chairman John Katko (R-NY)
Transportation Security and Counterterrorism and Intelligence Subcommittees
House Homeland Security Committee**

Safeguarding Our Nation's Surface Transportation Systems Against Evolving Terrorist Threats

Remarks as Prepared

I would like to welcome everyone to today's hearing.

I am pleased to be joined by my fellow New York delegation members Chairman Peter King, Ranking Member Kathleen Rice and Ranking Member Brian Higgins to talk about a topic that is so vital to the state of New York. Protecting our nation's surface transportation systems requires full cooperation and participation at the federal, state, local and individual levels.

An attack on any of our surface transportation systems would not only disrupt the local economy and infrastructure, but would have a ripple effect to cities across our nation.

For example, in my own district, in Syracuse, NY, we have a freight rail line that runs through our downtown area, and provides critical economic benefit to the region.

The purpose of today's hearing is to assess our ability and readiness to detect and disrupt threats to our nation's critical surface transportation systems.

Before we begin, I would like to express my pride and admiration for the four Americans that, through unrivaled acts of courage and bravery, were able to thwart a terrorist attack aboard a Paris-bound train on August 21, 2015.

The heroic actions of those four men; Mark Moogalian, a teacher originally from Midlothian, VA; Anthony Sadler, a senior at Sacramento State University; Air Force Airman 1st Class Spencer Stone and Oregon Army National Guard Specialist Alek Skarlatos, saved countless lives.

However, it is our responsibility to the American people to do all that we can to defend them against such heinous acts, and the American people should not be put in a position requiring them to defend their lives while riding a train, subway or bus to vacation, commute to work or simply run an errand.

Since September 11, 2001, many people have come to think of a terrorist attack against the United States as one which is an elaborate scheme against a hardened target.

Increasingly, however, the terrorists and their sympathizers are choosing soft targets; the Charlie Hebdo attack in Paris, the military recruiting centers attack in Chattanooga and now the train attack in Paris are just a few such examples.

I look forward to hearing from our witnesses today on their perspectives on the state of rail and mass transit security, to identify progress made since the terrorist attacks on September 11, 2001 and assess any remaining shortfalls.

###



OPENING STATEMENT

September 17, 2015

MEDIA CONTACTS

Susan Phalen, Matthew Ballard

**Statement of Subcommittee Chairman Peter King (R-NY)
Counterterrorism and Intelligence Subcommittee
House Homeland Security Committee**

“Safeguarding our Nation’s Surface Transportation Systems Against Evolving Terrorist Threats”

Remarks as Prepared

I would like to thank Chairman Katko for holding this joint hearing with the Counterterrorism and Intelligence Subcommittee today on terror threats to surface transportation.

With the recent attempt by a terrorist on a high-speed rail in Europe to take multiple lives, we are more cognizant than ever of the vulnerability of our public transportation infrastructure. That day, as Chairman Katko mentioned, passengers were fortunate to have among them four brave Americans—including two members of America’s armed forces—who reacted swiftly and bravely to take down the Islamist extremist who, armed with a rifle and ample ammunition, intended to take as many innocent lives as possible that day. But the odds are when the next would-be terrorist attacks passengers on a train or subway, the public may not be so fortunate as to have such capable and selfless persons on board and ready to react.

The easy access to rail transportation is one of the features that make it so popular. Compared with air travel, most of us individually appreciate the relative ease of using subways like the Metro here in DC or MTA in New York, or commuter rail, such as the MARC train in Maryland or the Long Island Railroad. Everyone values and enjoys simple and easy access. However, we have seen the vulnerability inherent in easy access in most mass transit services, including in attacks in London, Mumbai, Madrid, Tokyo, and now in Paris.

With ISIS urging supporters to carry out attacks in the U.S., we have to continuing evaluate the threat, vulnerability and related security measures within our surface transportation infrastructure.

I look forward to hearing from the witness about efforts to deter and prevent attacks, as well as how we are balancing the efficiency of public transit with security.

A key issue is how the Federal government is assisting state, local, and regional partners to better protect the traveling public against the threat of terrorism on America’s public transportation and commuter rail systems.

###

Statement of Eddie Mayenschein
Assistant Administrator
Office of Security Policy and Industry Engagement
Transportation Security Administration
U.S. Department of Homeland Security
before the
United States House of Representatives
Committee on Homeland Security
Subcommittee on Transportation Security
And
Subcommittee on Counterterrorism and Intelligence
September 17, 2015

Good afternoon Chairman Katko, Ranking Member Rice, Chairman King, Ranking Member Higgins, and distinguished Members of the Committee. I appreciate the opportunity to appear before you today to discuss the Transportation Security Administration's (TSA) role in surface transportation security.

TSA is a high-performing counterterrorism agency, applying a layered, intelligence-driven and risk-based approach to protect the Nation's transportation systems, including aviation, mass transit and passenger rail, freight rail, highway and motor carrier, and pipeline. Additionally, TSA leverages its core competencies in credentialing, explosives detection and intermodal security to support the U.S. Coast Guard as lead agency for maritime security. With its surface transportation programs, TSA strengthens and enhances the security of a complex

transportation network through cooperative and collaborative efforts with significant sector operators to develop best practices and share information.

Surface Transportation Background

TSA could not accomplish this essential mission without intelligence analysis and information sharing, explosives detection canine teams, Visible Intermodal Prevention and Response (VIPR) teams, and our industry partners voluntarily adopting security improvements and sharing best practices with each other and with TSA. This collaborative “whole community” approach helps to ensure that both TSA and industry resources are applied efficiently and have the highest efficacy in reducing risk to the Nation’s transportation systems.

Protecting the Nation’s transportation systems to ensure freedom of movement for people and commerce is crucial to every American’s daily life. There are over 12,000 individual companies or agencies that operate within the five modes of the surface transportation landscape. More than 500 individual freight railroads operate on nearly 140,000 miles of track carrying essential goods. Eight million large capacity commercial trucks, and almost 4,000 commercial bus companies travel on the four million miles of roadway in the United States and more than 600,000 highway bridges and through 350 tunnels greater than 100 meters in length. In the mass transit and passenger rail mode there are approximately 7,300 organizations representing a wide range of systems from very small bus-only systems in rural areas to very large multi-modal systems in urban areas. Surface transportation operators carry approximately 750 million intercity bus passengers and 10 billion passenger trips on mass transit each year. The pipeline industry consists of more than 2.5 million miles of pipelines, owned and operated by

approximately 3,000 private companies, which transport natural gas, refined petroleum products and other commercial products throughout the United States.

TSA oversees the development and implementation of risk-based security initiatives for these different modes of surface transportation in coordination with our security partners. As part of its security and counterterrorism mission, TSA works with private and municipal operator stakeholders to formulate policies and practices that improve security operations in their day-to-day environment. The Surface Division conducts analysis of transportation security and threat issues from both a long-term strategic perspective and near real-time analysis through data collected from TSA inspections and assessments. These analyses facilitate the assessment of risk in each surface mode and guide the development of risk reduction plans and initiatives. For instance, in 2007 our review of the industry scores in the training category of the BASE assessments indicated a potential vulnerability. TSA addressed this vulnerability by modifying the Transit Security Grants Program to prioritize front line employee training.

These activities, such as Security Awareness Messages (SAMs), provide our security partners with a menu of risk mitigation options they can implement based on the threat and their specific capabilities. Additionally, we develop, evaluate, approve, and implement surface transportation security initiatives to ensure that security guidance, policies, and regulations issued by TSA are risk-based, outcome-oriented, and effective in reducing risk.

Collaboration with Federal, State, Local, Tribal, and Private Entities

TSA maintains strong working relationships with modal administrations of the Department of Transportation (DOT). The Department of Transportation is the co-Sector Specific Agency with TSA for the transportation sector and routinely communicates, coordinates

and collaborates on the harmonization of safety and security priorities. This coordination includes working directly with the Federal Railroad Administration, the Federal Transit Administration, the Federal Highway Administration, the Federal Motor Carrier Safety Administration, and the Pipeline and Hazardous Materials Safety Administration. As part of the DHS-led Critical Infrastructure Partnership Advisory Council framework, DOT and TSA co-chair Government Coordinating Councils for surface transportation modes, including freight rail, mass transit and passenger rail, highway and motor carrier, and pipelines. Coordinated activities include collaboration on new and existing regulations, conducting security assessments and analysis of data, developing and conducting training and exercises to address counterterrorism and all-hazards, and sharing unclassified and classified information as appropriate.

TSA engages with state, local, tribal, and private sector partners to identify ways to reduce vulnerabilities, assess risk, and improve security through collaborative and voluntary efforts while maintaining the flow of people and commerce. Planning initiatives and policies in coordination with our stakeholders is of utmost importance. TSA works with industry operators to ensure efforts and resources are appropriately directed towards reducing risk to the surface transportation network and infrastructure. Collaboration with those stakeholders is particularly important, and achieved in part through formal structures like the DHS-led Critical Infrastructure Partnership Advisory Council framework, Sector Coordinating Councils, and other industry-centric organizations such as the Mass Transit Policing and Security Peer Advisory Group.

Through these established networks and other informal channels, TSA collaborates with security and corporate leadership of the industry and municipal operator stakeholders in the pursuit of policy that reduces risk, including implementation of exercises, physical and cyber hardening measures, and operational deterrence activities. We also work very closely with our

stakeholders in the development and dissemination of recommended practices, such as Security Action Items (SAIs) for mass transit, highway, and freight rail; motor-coach security best practices, and the Pipeline Security Smart Practice Observations. Through these networks, we have also established robust information sharing procedures and capabilities, such as the distribution of SAMs, the establishment of monthly stakeholder conference calls, and the dissemination of intelligence and threat information through modal Information Sharing and Analysis Centers (ISACs).

On the passenger rail side, TSA and Amtrak partner on programs such as Regional Alliance Including Local, State and Federal Efforts (RAILSAFE) to deter terrorist activity through unpredictable security activities. This program also incorporates other rail, transit, and local law enforcement agencies and involves counterterrorism activities such as increased station and right of way patrols, greater security presence on trains and at stations, explosive detection sweeps using canine teams, and random passenger bag inspections. Participating entities conduct these activities at local and regional high-risk transit locations to disrupt potential terrorist activities and reconnaissance as part of the layered approach to security. On average, more than 40 states and over 200 agencies, including TSA's VIPR teams, participate RAILSAFE activities.

Through highway and motor carrier security programs, TSA has provided multiple voluntary initiatives to industry through forums and other communications, including security action items and training, which focus on over-the-road buses that service high threat urban areas, trucks carrying hazardous materials, and student transportation. Additionally, TSA coordinates and collaborates with the Department of Transportation to develop and implement a National Strategy for Bridge and Tunnel Security based on the United States Army Corps of

Engineers' (USACE) vulnerability assessments. As a result, and working with USACE, TSA has assessed 100 percent of all high-risk bridges and tunnels, and has provided 81 percent of the remediation recommendations to asset owners. The final 19 percent of reports are in the process of being completed and will be shared within the next twelve months.

For the transport of hazardous cargo on the nation's roadways, TSA conducts security threat assessments on professional drivers with Commercial Drivers Licenses who seek endorsement to haul hazardous materials. Only those applicants who have been successfully vetted and have received a TSA-approved Security Threat Assessment (STA) are allowed to transport such hazardous materials.

We work very closely with the pipeline industry on identifying and improving cybersecurity vulnerabilities, including coordinating a number of classified briefings to increase awareness of the threat. TSA's involvement in the Pipeline Corporate Security Review (CSR) and Critical Facility Security Review (CFSR) program continues to help our pipeline stakeholders improve their organization-wide and critical infrastructure-specific security postures.

As an example of our close working relationships with the industry, TSA recently successfully launched the Loaned Executive Program aimed at providing senior level transportation security officials with first-hand experience of the Transportation Security Administration's various counter-terrorism and risk reduction roles in enhancing industry security is providing real-world experience and detailed industry exposure to TSA's surface security programs and policies. The program, which began as a pilot last September, has seen executives from Amtrak, Washington Metropolitan Area Transit Authority and Bay Area Rapid Transit Authority participate in the program so far.

TSA provides the Federal Emergency Management Agency (FEMA) with subject matter expertise to assist in the development of transportation security Notice of Funding Opportunities (grants) for surface transportation owners and operators. These FEMA grants support transportation risk mitigation by applying federal funding to critical security projects with the greatest security effects. Between fiscal years 2006 and 2014, over \$2.2 billion in transportation security grant funding was awarded to freight railroad carriers and operators, over-the-road bus operators, the trucking community, and public mass transit owners and operators, including Amtrak, and their dedicated law enforcement providers. TSA continuously reviews the grant program framework and makes recommendations to FEMA, ensuring funding priorities are based on identified or potential threat and vulnerabilities identified through TSA assessment programs such as the Baseline Assessment for Security Enhancement (BASE) program, together with consideration of potential consequences. As a result, DHS is able to direct grant funds to activities that have the highest efficacy in reducing the greatest risk, such as critical infrastructure vulnerability remediation, equipment purchases, anti-terrorism teams, mobile screening teams, explosives detection canine teams, training, drills/exercises, and public awareness campaigns.

Training and Exercises

TSA works closely with our transportation stakeholders to provide resources for security training and exercises. Through a national review of assessments, TSA identified areas where we could assist transportation entities in providing better security training to their frontline employees. As such, TSA prioritized the development and distribution of security training resources for surface transportation frontline employees through channels such as TSA-produced

training modules and making recommendations to adjust grant program priorities. TSA's First Observer™ program trains highway professionals and other security entities, such as those responsible for providing parking and facility security at major sporting arenas and venues, to observe, assess, and report potential security and terrorism incidents. Since FY 2006, over \$141 million in grant funding has been awarded to mass transit, freight rail, and over-the-road bus operators for security training, including over \$129 million through the Transit Security Grant Program for mass transit agencies and Amtrak; over \$6.9 million through the Freight Rail Security Grant Program for freight rail carriers; and \$5.4 million through the Intercity Bus Security Grant Program for over-the-road bus operators. Additionally, we have developed and distributed an array of mode-specific training products for frontline employees. With this targeted effort on security training, TSA has seen assessment results related to security training improve across all modes of surface transportation. As an example, since 2007, the percentage of grant-eligible mass transit agencies that have a sound security training program based on their BASE scores has increased from 19% to 66%. Also, as a sub-set, the percentage of agencies in the higher-risk regions with sound security training programs has increased from 27% to 78%.

With regard to exercises, TSA collaborates with industry through our Intermodal Security Training and Exercise Program (I-STEP) across all modes of surface transportation. TSA facilitates I-STEP exercises to help surface transportation entities test and evaluate their security plans, including prevention and preparedness capabilities, and their ability to respond to threats and cooperate with first responders from other entities. Entities that receive an I-STEP exercise are selected through an extensive review process based on risk, which looks at elements such as assessment results, emerging threats as identified through intelligence resources. As new threats

emerge, I-STEP scenarios are updated to ensure our industry partners are prepared to exercise the most appropriate countermeasures.

Assessments and Inspections

TSA also plays a role in surface transportation security through voluntary assessments and regulatory compliance inspections. The Surface Division works closely with TSA's Office of Security Operations (OSO), which conducts both voluntary assessments and required regulatory compliance inspections.

TSA conducts approximately 10,000 regulatory inspections of freight railroads each year to ensure compliance with regulations requiring the secure exchange of custody of rail cars carrying Rail Security Sensitive Materials, as well as reporting significant security concerns and providing location and shipping information of certain rail shipments to TSA.

OSO's Surface Transportation Security Inspectors conduct a thorough security program assessment of mass transit agencies to include Amtrak, and over-the-road bus operators through the BASE program. BASE assessments are conducted with emphasis on the 100 largest mass transit and passenger railroad systems measured by passenger volume, which account for over 95 percent of all users of public transportation. Results of these assessments feed into resource allocation decisions, including I-STEP exercises and grant funding, to ensure that the higher-risk entities with the greatest need receive priority consideration for available resources. For instance, in 2007 our review of the industry scores in the training category of the BASE assessments indicated a potential vulnerability. TSA addressed this vulnerability by modifying the Transit Security Grants Program to prioritize front line employee training.

Assessments and inspections in surface transportation are not limited to rail and highway operations. In pipeline mode, for example, the Implementing Recommendations of the 9/11 Commission Act of 2007 (Pub. L. No. 110-53) required TSA to develop and implement a plan for inspecting the critical facilities of the top 100 pipeline systems in the nation. These required inspections were conducted between 2008 and 2011 through the Critical Facility Inspection program, with regular recurring reviews now being conducted through TSA's Critical Facility Security Review program.

Conclusion

TSA works collaboratively with surface transportation industry partners to develop and implement programs while enhancing security and mitigating the risk to our Nation's surface transportation systems while promoting commerce. I want to thank the Committee for its continued assistance to TSA and for the opportunity to discuss our work in partnering with the surface transportation industry to provide better security to the American people. Thank you, and I look forward to your questions.



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

DRAFT

SURFACE TRANSPORTATION SECURITY

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

Notice:
This draft is
restricted to official
use only.

This draft report is being provided to obtain advance review and comment. It has not been fully reviewed within GAO and is subject to revision.

Recipients of this draft must not, under any circumstances, show or release its contents for other than official review and comment. It must be safeguarded to prevent improper disclosure. This draft and all copies remain the property of, and must be returned on demand to, the Government Accountability Office.

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.

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

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.



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

¹The 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.

²Pub. 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

³Pub. 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.

⁴GAO, *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

⁵Pub. 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

⁶49 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.

⁷49 C.F.R. § 1580.5.

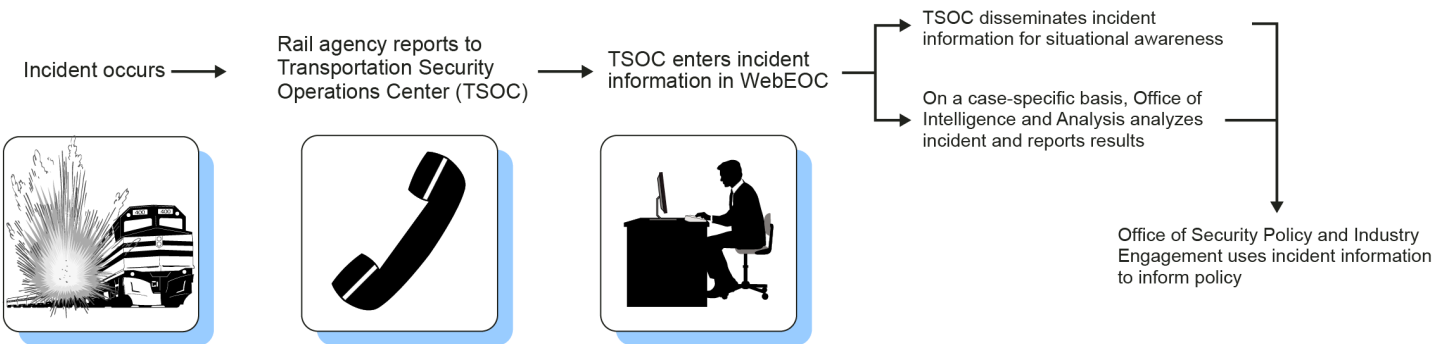
⁸71 Fed. Reg. 76,852, 76,876 (Dec. 21, 2006).

⁹49 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

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.

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

¹⁰There 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.

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

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. 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

¹²According 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.

¹³Sixty-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.

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 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

¹⁴These 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.

¹⁵GAO-13-20.

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.

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

¹⁶GAO-13-20

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

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

¹⁷For 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.

¹⁸This 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.

¹⁹We 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.

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 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 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

²⁰GAO-13-20.

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

²²To 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.

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 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.

**Testimony before the U.S. House of Representatives
Committee on Homeland Security's
Transportation Security and Counterterrorism and Intelligence Subcommittees
Metropolitan Transportation Authority Director of Security Raymond Diaz
Thursday, September 17, 2015, 2 p.m.**

Good afternoon Chairmen Katko and King, and other members of the subcommittees. Thank you for holding this hearing and for inviting me to discuss security at New York's Metropolitan Transportation Authority. Joining me today are Michael Coan, Chief of Department of the MTA Police.

Before joining the MTA in January 2014 as Director of Security, I served as Chief of the New York City Police Department's Transit Bureau, responsible for the safety and security of the MTA New York City Transit system. During my 41-year career with the NYPD, I also served as commanding officer of Patrol Boroughs Manhattan North and South, and the School Safety Division. Before joining the NYPD, I served in Vietnam with the U.S. Marine Corps.

In my present position, I'm responsible for the security of the MTA, including coordinating MTA efforts with the Department of Homeland Security, the FBI, the National Guard, the NYPD, and the New York and Connecticut State Police. I oversee the MTA Police Department, which has jurisdiction in 14 counties in New York and Connecticut and patrols a 5,000-square mile rail network. I'm responsible for the implementation and execution of a security strategy that offers maximum protection to the public, MTA employees, and MTA property.

Before I discuss security in more depth, I'd like to set the stage with some basic facts about the MTA. Every day, we move more than 8.7 million people on our subways, buses, and commuter rail lines. We're one of the few transit systems in the world that operates 24 hours a day, seven days a week, 365 days a year. Our seven bridges and two tunnels carry nearly 300 million vehicles a year. Our network of trains, buses, bridges, and tunnels is a one trillion dollar asset, meaning this: If we were to build our network today—including about 9,000 railcars, 5,000 buses, and millions of other assets—it would cost nearly one trillion dollars.

Protecting millions of people a day and a trillion dollar asset is an enormous task. I can tell you that the MTA's top priority is clear: Ensuring the safety and security of our customers and employees. To protect our customers and our assets, the MTA employs a multi-layered security strategy. Some strategies, like policing, are highly visible; others are less visible, like structural hardening, advances in technology, and improved communications.

The hallmark of policing our 5,000 square-mile territory is collaboration. Let me explain. The NYPD is responsible for patrolling the most heavily-used portion of our network, New York City subways and buses. We work closely with the NYPD to ensure that capital investments are consistent with the latest security and policing strategies.

The MTA PD polices our commuter rail system. Metro-North Railroad and Long Island Rail Road are the two busiest commuter rail agencies in the country. Since 9/11, we've concentrated on counter-terrorism strategies. The department has grown from 494 uniformed officers to 722 today. Fifty K9 teams are now deployed throughout the system, and we've significantly increased our presence on trains and at stations. In addition to the MTA PD, 721 Bridge and Tunnel officers patrol our seven bridges and two tunnels.

In response to the growing threat of active shooter attacks, over 95% of our MTA PD officers have received TSGP-funded Active Shooter Training. In addition, over 60 officers have received heavy weapons training.

We have a robust “See Something, Say Something” campaign, coupled with security awareness training for civilian front-line employees. The two serve to encourage vigilance as well as educate individuals as to what appropriate action should be taken when suspicious activity is observed. To date, the MTA has trained in excess of 35,000 front-line employees.

The recent incident of a potential active shooter in France thwarted by vigilant rail passengers clearly illustrates the importance of such awareness initiatives and training. TSGP grant awards have also supported our “See Something, Say Something” campaign and civilian employee training.

Behind the scenes, one critical layer to our security is the structural and technological hardening of our infrastructure. Since 9/11, the MTA has invested close to \$1.4 billion of local funds toward an aggressive campaign to harden our subway and commuter rail systems, as well as bridges, tunnels, and other infrastructure. Critical stations and vulnerable areas have been secured with electronic security systems consisting of CCTV, intrusion detection, and access control devices. We’ve also deployed chemical, biological, and radiological detection technology at such locations.

We’ve benefitted from over \$400 million dollars in support of our security program from DHS since 2003. TSA and FEMA have helped us immeasurably with grant allocations and reallocations. Unfortunately the trend of a shrinking national program has limited our ability to move forward with our capital security mitigations. For example, in FY2009 the MTA received \$92 million of a \$349 million national program. Six years later, the national appropriation has dropped by 75%, leaving only \$87 million for transit agencies across the country.

We’re grateful for this support, and are pleased that the initial “period of performance” for transit security grants has been extended to 36 months, which affords us the time needed to complete capital security projects funded through the TSGP.

Another layer of the MTA’s security strategy is communication and intelligence sharing. At the federal level, we have an excellent working relationship with our DHS partners, represented by FEMA and TSA. We attend regular meetings and conference calls, and continually exchange information. When potential threats are identified, they are communicated immediately.

We share intelligence with many law enforcement agencies, on a daily basis, through our Inter-Agency Counterterrorism Task Force (ICTF). Additionally, we conduct joint patrol initiatives with other regional transportation agencies including: Amtrak, the Port Authority of New York and New Jersey, New Jersey Transit, the New York and Connecticut State Police, the New York State National Guard, and the NYPD.

MTA PD detectives represent the MTA on the FBI’s Joint Terrorism Task Force, the FBI Cyber Crimes Unit, the High Intensity Drug Trafficking Area program, and the NYPD Counter Terrorism and Intelligence units.

I’m proud to oversee this system and its proactive and accomplished security personnel, and look forward to continuing to work with my colleagues in law enforcement and you in the House

to keep our customers safe and our system secure. Once again, thank you for inviting me to testify today. I'm happy to answer any questions you might have.

**TESTIMONY OF
POLLY HANSON
CHIEF OF POLICE
NATIONAL RAILROAD PASSENGER CORPORATION
60 MASSACHUSETTS AVENUE, NE
WASHINGTON, DC 20002**

**BEFORE THE
HOUSE COMMITTEE ON HOMELAND SECURITY
SUBCOMMITTEE ON TRANSPORTATION SECURITY
AND
SUBCOMMITTEE ON COUNTERTERRORISM
AND INTELLIGENCE**

**HEARING ON
“SAFEGUARDING OUR NATION’S SURFACE
TRANSPORTATION SYSTEMS AGAINST
EVOLVING TERRORIST THREATS”**

**THURSDAY, SEPTEMBER 17, 2015
2:00 P.M.
311 CANNON HOUSE OFFICE BUILDING**

Chairmen Katko and King, Ranking Members Rice and Higgins, and members of the Subcommittee, good afternoon, and thank you very much for the invitation to testify today. Amtrak takes its responsibility to protect its riders very seriously, and on behalf of Mr. Boardman, our President and CEO, and the men and women of the Amtrak Police Department (APD) I welcome the opportunity to testify before you today.

Amtrak is America's Railroad. Our passengers travel between more than 500 communities in 46 states and our trains operate on over 21,000 miles of track. Amtrak operates more than 300 daily trains delivering over 30 million travelers a year safely to their destinations. The Amtrak Police Department was created to protect Amtrak's employees, passengers, patrons, stations, stops, rolling stock, and other critical infrastructure. We do that by working closely with our colleagues in the law enforcement and counter-terrorism communities to collect intelligence, pilot new technology, and surge our resources on Amtrak trains, along our right-of-ways, and in our stations and engage our passengers and patrons in being our partners in safety.

The Amtrak Police Department consists of more than 500 members based in 30 locations. While the Department was created in the 1970's, it really wasn't until after September 11 that counter-terrorism became a large focus of our security plans. Uniform Patrol Division officers are the most visible part of our department. They patrol stations, ride trains, perform education and enforcement on railroad safety, and are the first response to Amtrak incidents. Our Special Operations Unit consists of officers with tactical skills who perform station surges, conduct random passenger bag screening, and perform counter surveillance, right-of-way patrols, and dignitary protection. Our K-9 program which consists of both conventional and vapor wake detection dogs average 1,000 train rides a month. The Transportation Security Administration (TSA) supports Amtrak's robust K-9 program.

Terrorist tactics continue to evolve, and we must keep pace. U.S. based extremists will continue to pose the most frequent threat to the U.S. Homeland. As the tragic attacks in Boston, Texas, and New York have shown over the last several years, the new terrorist threats are already here. Either alone or in small groups, with the ability to mask the extent of their radicalization, these individuals represent the most lethal of threats. From “lone wolf” attackers to ISIL radicals, we see a greater likelihood of attack than we have in years. The internet and cyberspace has become the new recruiting ground and the new battlespace. Aided by the internet and social media, ISIS has featured plans to kill U.S. soldiers or law enforcement and the recent attacks in France and against tourists in Tunisia demonstrate the threat is increasing.

Across the country, we coordinate with numerous other local, state, and Federal agencies, including the TSA, DHS, NCTC, CBP, DEA, FBI, U.S. MARSHALLS and the U.S. Capitol Police. Amtrak officers are assigned to the FBI National Joint Terrorism Task Force at the National Counter-Terrorism Center, as well as Joint Terrorism Task forces in Baltimore, Chicago, New York, Philadelphia, Boston, and Washington, D.C.

One of our most visible efforts builds on a partnership with the TSA that led to the creation of the Regional Alliance Including Local, State, and Federal Efforts (RAILSAFE) Network. More than 200 agencies in over 40 states usually participate in Operation RAILSAFE which increases visibility at stations and stops and along the right-of-way and by water and in the air. Amtrak Police, NYPD, and TSA started RAILSAFE in 2010 and there have been 50 RAILSAFEs in 42 states, the District of Columbia, and Vancouver, Canada involving over 265 agencies and over 1,600 law enforcement members since then.

Amtrak has used DHS funding to provide our RAILSAFE partners and other first responders with training on railroad safety, the sharing of intelligence, and the unified

response to Amtrak incidents. This training has been provided to almost 300 participants since 2014 in 11 states.

Internationally, Amtrak Police has partnered with foreign rail law enforcement agencies throughout Europe with the RAILPOL organization. Rail policing issues, intelligence, and information sharing are discussed and solid relationships have been established by our participation. Additionally, Amtrak Police has a working relationship with Interpol.

Building on the extensive intelligence, military, and law enforcement backgrounds of its members, the Amtrak Intelligence Unit coordinates with the United States Department of Transportation Office of Intelligence, Security, and Emergency Response and has members aligned with the Washington Regional Threat Analysis Center and the Maryland State Fusion Center. Amtrak Police also welcome the Visible Intermodal Protection and Response (VIPR) Teams who deploy at many of our station facilities on an unpredictable and random basis. On a daily basis, TSA supports Amtrak's random passenger bag inspection program.

Amtrak is a DHS test bed for the piloting of new technology and we have taken advantage of the TSA Surface Transportation Security Inspection Program Baseline Assessment for Security Enhancement, which highlights Amtrak's security posture and adherence to accepted security practices.

To extend our reach, we have developed programs that enable other Amtrak employees as well as our passengers to report on things that strike them as unusual or suspicious. We have trained Amtrak's employees in techniques to spot suspicious behaviors. Using phones or texting, these tools have added tens of thousands of eyes to our efforts to watch over our passengers, trains, and facilities. The ability to leverage our skilled workforce, with its knowledge of the operating environment, is an important strength that contributes to the security and safety of our system. It is part of our larger strategy

of working collaboratively with partner organizations and passengers so that we can add their unique strengths to our own to ensure the safety of our system and the communities it serves.

Amtrak has taken advantage of DHS public awareness campaigns like “If You See Something, Say Something” and texting a tip to APD11 which was another initiative supported by DHS funding. I want to emphasize that since the creation of TSA there have been many security measures implemented but we need to continue our partnerships, encourage our employees, passengers, and patrons to be observant and report suspicious activity or behavior.

Thank you again, for this opportunity to discuss the Amtrak Police role in rail passenger and infrastructure protection. I look forward to answering any questions that you may have.