United States Government Accountability Office

Report to Congressional Requesters

September 2019

SURFACE TRANSPORTATION

DHS Is Developing and Testing Security Technologies, but Could Better Share Test Results

GAO-19-636

September 2019

SURFACE TRANSPORTATION

DHS Is Developing and Testing Security Technologies, but Could Better Share Test Results

GAO Highlights

Highlights of GAO-19-636, a report to congressional requesters

Why GAO Did This Study

Since 2016, bombings of subways and bus systems in foreign cities and attempted attacks in U.S. cities demonstrate continued security threats to mass transit and other surface transportation systems. S&T and TSA are the primary federal entities responsible for researching, developing, and testing technologies designed to address threats to these systems. GAO has previously identified challenges with S&T's oversight of R&D projects.

GAO was asked to review S&T and TSA's roles in developing and testing surface transportation security technologies. This report, among other objectives, (1) assesses the extent to which S&T is developing technologies to secure surface transportation systems and progress made, and (2) identifies the key mechanisms that S&T, TSA, and stakeholders use to collaborate and share information on identifying capability gaps and security technologies, and analyzes the extent to which they are effective.

GAO assessed S&T's mass transit program because it was the only active R&D effort for surface transportation security. GAO interviewed officials from S&T, TSA, and nine mass transit operators; observed technologies; reviewed documentation; and analyzed budget information from fiscal years 2013 to 2018. GAO also used GAO's leading collaboration practices to assess collaboration on security technologies.

What GAO Recommends

GAO is making two recommendations: that S&T incorporate DHS milestone guidance for its STETD program, and that TSA develop a mechanism to routinely and comprehensively share security technology information with mass transit operators. DHS concurred with both recommendations.

View GAO-19-636. For more information, contact William Russell at (202) 512-8777 or russellw@gao.gov

What GAO Found

The Department of Homeland Security's (DHS) Science and Technology Directorate (S&T) has one research and development (R&D) effort focused on surface transportation, the Surface Transportation Explosive Threat Detection (STETD) program, which is developing technologies to secure mass transit systems (see figure). DHS guidance requires S&T to develop results-oriented milestones to track progress. GAO found, however, that S&T has not used milestones that fully adhered to DHS guidance. For example, most STETD program milestones did not clearly link to key activities described in program plans. As a result, DHS may not have the information needed to determine whether the STETD program is meeting its goals.

Examples of Technologies DHS S&T Is Developing to Secure Mass Transit

Standoff Detection
A set of imaging sensors designed to scan crowds for hidden threat items on travelers.

Real-Time Threat Detection
Technology intended to automatically detect abandoned items that could be threats.

Source: Department of Homeland Security (DHS) Science and Technology Directorate (S&T). | GAO-19-636

S&T, TSA, and stakeholders effectively collaborate, but TSA could better share test results with mass transit stakeholders. For example, S&T, TSA, and mass transit operators regularly collaborate on issues related to identifying mass transit capability gaps and testing security technologies to address those gaps. Nevertheless, GAO found TSA's efforts to share information on existing technologies to secure mass transit could be improved. Specifically, TSA regularly assesses commercially available technologies, but does not routinely or comprehensively share its results with mass transit operators. For example, TSA's reports on its testing of commercially available products would provide mass transit operators with technical assessment information. However, seven of the nine mass transit operators GAO spoke with asked for more technical assessment information on existing commercial technologies, indicating that they may not be receiving the TSA products that would provide this information. Sharing this information more routinely and comprehensively with mass transit operators would allow TSA to better inform them about the capabilities of technologies that could be acquired to secure thteir systems.

Contents

Abbreviations

DHS	Department of Homeland Security
FOVEA	Forensic Video Exploitation and Analysis
IED	improvised explosive device
IPT	Integrated Product Team
RDWG	Intermodal Transportation Systems Research and Development Working Group
R&D	research and development
S&T	Science and Technology Directorate
STETD	Surface Transportation Explosive Threat Detection
PAG	Transit Policing and Security Peer Advisory Group
TSA	Transportation Security Administration

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

September 12, 2019

Congressional Requesters,

Since 2016, bombings of subway and bus systems in foreign cities such as Brussels and St. Petersburg, as well as planned attacks in the New York City area and other U.S. cities, demonstrate the persistence of security threats to surface transportation systems. Surface transportation systems generally rely on an open infrastructure that is difficult to monitor and secure due to its multiple access points, hubs serving multiple carriers, and in some cases, lack of access barriers. Mass transit systems are one component of the nation's surface transportation system, which also includes freight rail, highways, and pipelines, among other modes.[1] Given the inherent difficulty of securing mass transit and other surface (or land) transportation systems, federal, state, local, and mass transit officials rely on research and development (R&D) to identify or produce potential technology solutions to address security vulnerabilities.

Within the federal government, the U.S. Department of Homeland Security's (DHS) Science and Technology Directorate (S&T) and Transportation Security Administration (TSA) are the primary entities responsible for researching, developing, and testing technologies designed to address risks facing surface transportation systems. Specifically, S&T is the primary component within the department responsible for R&D of security technologies, as well as coordinating and integrating all such activities of the department.[2] TSA is responsible for ensuring the security of all modes of transportation in coordination with other federal entities, state and local governments, and the private sector,

[1]Mass transit systems include terminals, operational systems, and supporting infrastructure for passenger services by transit buses, trolleybuses, monorail, heavy rail (also known as subways or metros), light rail, commuter rail, and vanpool/rideshare. A mass transit bombing occurred in Brussels, Belgium on March 22, 2016, and in St. Petersburg, Russia on April 3, 2017. There have been multiple thwarted attacks against New York mass transit, including undetonated explosives that were found in a trash receptacle near a mass transit station in Elizabeth, New Jersey on September 18, 2016.

[2]See Pub. L. No. 107–296, § 302, 116 Stat. 2135, 2163-64 (2002) (codified at 6 U.S.C. § 182). As of September 2018, seven DHS components have budget authority to conduct R&D activities—S&T, the Coast Guard, the Countering Weapons of Mass Destruction Directorate, the U.S. Secret Service, the Cybersecurity and Infrastructure Security Agency, TSA, and the Office of the Chief Information Officer within the Office of the Undersecretary of Management.

including surface transportation systems.[3] We have previously identified challenges with S&T's coordination and oversight of R&D projects. Specifically, in March 2019, we reported that R&D coordination across DHS had improved, but additional actions were needed to better track and evaluate S&T R&D projects.[4]

Given DHS's past challenges managing R&D projects and the inherent difficulties associated with monitoring and securing surface transportation systems, you asked us to review federal R&D efforts to develop technologies that strengthen security within the surface transportation environment. This report (1) assesses the extent to which S&T is developing technologies to secure surface transportation and what progress it has made; (2) describes the extent to which TSA is testing technologies to secure surface transportation; and (3) identifies the key mechanisms that S&T, TSA, and stakeholders use to collaborate on surface transportation capability gaps and share information on relevant security technologies, and analyzes the extent to which they are effective.

To assess the extent to which S&T is developing technologies to secure surface transportation and its progress to date, we identified all S&T related efforts since 2010, when S&T began a research initiative focused on surface transportation security technologies. We focused this review on mass transit security because it was the only active S&T R&D effort related to surface transportation since 2010. To collect information on technologies developed we reviewed S&T documentation, including technology performance reviews and project developmental milestones, interviewed agency officials, and visited one of the nation's largest mass transit operators that was testing an S&T-developed technology. We reviewed prior GAO reports on S&T's management of R&D projects to identify prior findings applying to S&T's broader R&D portfolio that may

[3]In response to the attacks of September 11, 2001, the Aviation and Transportation Security Act (ATSA) was enacted, creating TSA and giving it responsibility for security in all transportation modes. Pub. L. No. 107-71, § 101(a), 115 Stat. 597, 597 (2001) (codified at 49 U.S.C. § 114).

[4]For example, we found that S&T used disparate information sources to identify and track R&D project information and faced challenges in tracking progress and other information for ongoing R&D projects. As of August 2019, DHS had not completed actions to address our 2019 recommendation to better track and evaluate projects using leading practices in DHS's budget preparation guidance. See GAO, *Homeland Security: Research & Development Coordination Has Improved, but Additional Actions Needed to Track and Evaluate Projects*, GAO-19-210 (Washington, D.C.: Mar. 21, 2019).

also apply to S&T's management of its mass transit R&D program.[5] In addition, to better assess how S&T has managed challenges related to its R&D program for mass transit security, we assessed S&T's program milestones that were reported to Congress for each fiscal year from 2013 through 2018 against DHS budget guidance for developing milestones.[6]

To describe the extent to which TSA has tested surface transportation security technologies, we reviewed agency documentation pertaining to tested technologies, TSA budget information for fiscal years 2013 through 2018 (the most recent 5 year period when we initiated our work), and interviewed agency officials.[7] We also conducted two site visits to mass transit operators to observe the testing and use of security products.[8] We focused our site visits on mass transit operators because TSA officials told us they prioritize this mode over other surface transportation modes when determining what to test. We selected mass transit operators for site visits to obtain a variation in the type of commercial technologies being tested.

To analyze the key mechanisms S&T, TSA, and stakeholders use to collaborate on surface transportation capability gaps and share information with each other on relevant security technologies, we focused on mass transit operators because S&T and TSA have focused their respective R&D and testing efforts on technologies designed to enhance the security of mass transit systems. We identified mechanisms used by S&T, TSA, and mass transit stakeholders (including operators and industry associations) to promote collaboration on security-related issues. We reviewed documentation related to these mechanisms, and interviewed agency officials and mass transit stakeholders that held memberships in these groups or participated in these processes. We

[5]See GAO-19-210 and GAO, *Department of Homeland Security: Oversight and Coordination of Research and Development Should Be Strengthened*, GAO-12-837 (Washington, D.C.: Sept. 12, 2012).

[6]For DHS guidance, see Department of Homeland Security, *DHS Budget Build Framework* (Washington, D.C.: Revised November 14, 2017).

[7]Specifically, we reviewed final program budget information for the Surface Transportation Operational Test Bed Program provided by TSA program officials.

[8]We visited the Metropolitan Atlanta Rapid Transit Authority and the Los Angeles County Metropolitan Transportation Authority.

evaluated these mechanisms against leading collaboration practices.[9] To determine the extent to which information is shared on security technologies, we assessed TSA's efforts to share information because it has responsibility for securing surface transportation and, thus has established relationships with mass transit operators. We did not assess S&T's information sharing with mass transit operators because S&T primarily interacts with operators based on their participation in TSA's testing program for surface transportation technology products. We conducted semi-structured interviews with nine mass transit operators on TSA's efforts to share information. For these interviews, we selected operators to reflect a variation in the size of transit systems, geographic location, and membership in certain groups that promote collaboration on mass transit security issues.[10] Further, we reviewed documentation and interviewed TSA officials on their efforts to share information on security technologies with mass transit operators. We assessed these information sharing efforts against federal internal control standards and criteria within DHS's *National Infrastructure Protection Plan.*[11]

We conducted this performance audit from April 2018 to September 2019 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.

[9]See GAO, *Managing for Results: Key Considerations for Implementing Interagency Collaborative Mechanisms*, GAO-12-1022 (Washington, D.C.: September 2012), which identifies leading practices that should be used to effectively implement collaborative mechanisms, such as collaborative groups. Specifically, we evaluated a particular mechanism against those practices that were most relevant. In cases where we did not assess a mechanism against all the practices, we provided a justification within the body of this report.

[10]To make our selection of transit operators based on size, we used data on transit system ridership collected by the American Public Transportation Association. Also, with respect to participation in certain groups, we considered whether the mass transit systems were members of the Transit Policing and Security Peer Advisory Group, the Intermodal Transportation Systems Research and Development Working Group, and the Surface Transportation Operational Test Bed Program. We discuss these groups later in our report.

[11]GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: September 2014). Department of Homeland Security, *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: December 2013).

Background

Securing the Mass Transit Environment

Mass transit rail operators have primary responsibility for securing their own systems. Unlike the aviation environment, where TSA has operational responsibility for screening passengers and baggage for prohibited items prior to boarding a commercial aircraft, TSA has no operational role for securing mass transit, such as employing screeners or purchasing and acquiring security equipment.[12] Rather, TSA regularly partners with mass transit operators to address their security needs by conducting vulnerability assessments, sharing intelligence information and best practices, and working to mitigate security risks to their systems by assessing commercially available security technologies, among other measures.[13] Mass transit operators which can be public or private entities, administer and manage all transit activities and services, including acquiring and operating any technologies designed to augment their existing security infrastructure.

Securing transit systems presents inherent challenges for mass transit operators for numerous reasons. In general, mass transit systems are designed to expedite the movement of large numbers of people through multiple stations, situated along extended routes, and technologies used in the mass transit environment should not disrupt the efficiency of these operations. In addition, individual stations within these systems frequently include multiple points of entrance and exit that vary in the extent to which they may be accessed by passengers. For example, open systems include walk-up platforms with little to no barrier to entry, while other, more closed systems, typically include dedicated points of entry and exit that allow or prohibit entry access through various mechanisms. Given the size and complexity of these systems, it can be difficult for operator personnel to comprehensively monitor them for security threats. Finally,

[12]However, while TSA has no operational role, they do partner with mass transit operators through the Visible Intermodal Prevention and Response program to augment high visibility patrols with mass transit operators as a force multiplier.

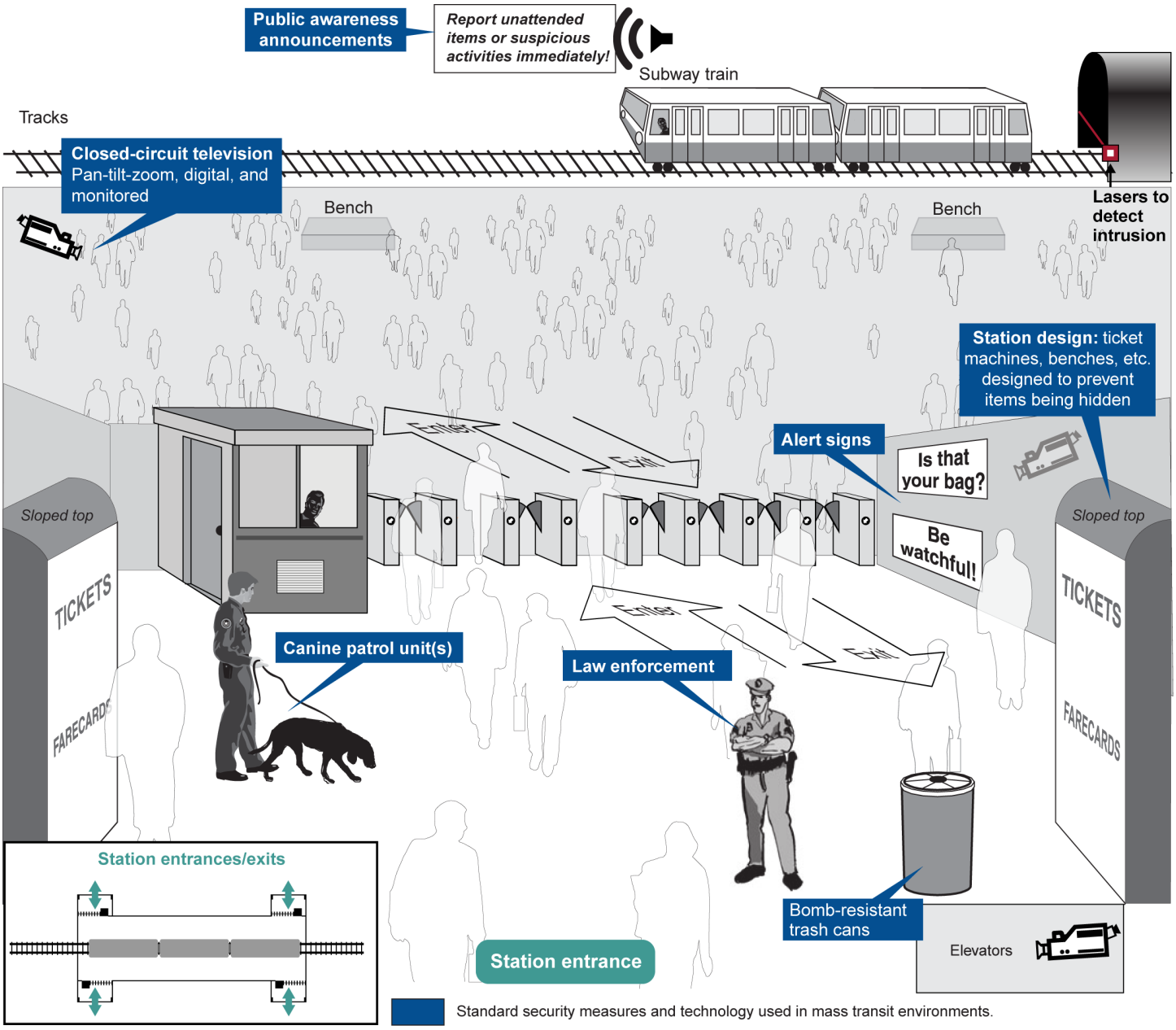
[13]TSA has issued a few requirements for mass transit operators, including that rail carriers designate a rail security coordinator and a designated backup who is consistently available to TSA. Rail security coordinators are to serve as the primary contact for receipt of intelligence information and other security-related activities for passenger rail agencies. See 49 C.F.R. § 1580.201. Rail carriers also must immediately report potential threats and significant security concerns to DHS. See 49 C.F.R. § 1580.203.

the large number of riders that pass through these systems during peak hours generally makes the sustained use of some security measures and technologies (e.g., metal detectors) difficult because such measures could result in long lines that would disrupt scheduled service.

Though mass transit systems are difficult to secure, mass transit operators commonly employ a number of standard security measures for the transit environment, including:

- public awareness announcements and signage (e.g., reminders to report unattended baggage or suspicious activities to operator personnel immediately);
- visible security personnel;
- use of canine teams;
- access controls, such as the use of lasers for intrusion detection;
- station design (e.g., designing transit stations to limit recess areas where bombs could be hidden, such as under a bench or a ticket machine); and
- video surveillance, which includes video cameras that transmit a signal to a set of television monitors to display real-time footage of transit system platforms, entrances, exits, etc. (see figure 1).

Figure 1: Security Measures Commonly Used in the Mass Transit Environment



Source: GAO analysis of Department of Homeland Security information; Art Explosion (clip art). | GAO-19-636

Requirements, Roles, and Responsibilities for Mass Transit R&D

Federal requirements for mass transit R&D efforts guide department and agency efforts. Specifically, the Implementing Recommendations of the 9/11 Commission Act of 2007 requires that S&T, in consultation with TSA and the Federal Transit Administration, carry out an R&D program to improve the security of public transportation systems.[14] Additionally, Executive Order 13416, *Strengthening Surface Transportation Security,* requires the Secretary of Homeland Security to coordinate research, development, testing, and evaluation of technologies related to the protection of surface transportation, including commercial off-the-shelf products.[15] To implement these requirements and other related activities to help secure mass transit systems, DHS, S&T, and TSA, in coordination with mass transit operators, have assumed the following roles and responsibilities:

DHS. DHS carries out its requirement to coordinate department-wide R&D (including that for mass transit and other surface transportation modes) through its Integrated Product Team (IPT) process.[16] The IPTs themselves are comprised of officials across DHS components, and are tasked with identifying DHS technology capability gaps, which are defined as differences between a department or agency's current capabilities and those capabilities needed to perform its mission. Each IPT is responsible for identifying capability gaps related to a broad security area (such as preventing terrorism) and potential R&D efforts to address those gaps.[17] Capability gaps relevant to surface transportation, including mass transit, fall under the Prevent Terrorism IPT and its Explosive Screening sub-IPT. S&T's Research Council receives IPT information on security gaps and is responsible for prioritizing them across all IPTs. The results are used to inform which R&D research projects S&T and DHS components will undertake (see figure 2).[18]

[14]See Pub. L. No. 110–53, § 1409, 121 Stat. 266, 411 (2007) (codified at 6 U.S.C. § 1138). The Federal Transit Administration oversees safety of rail transit systems that typically serve individual metropolitan areas, using track not shared with freight and other passenger trains.

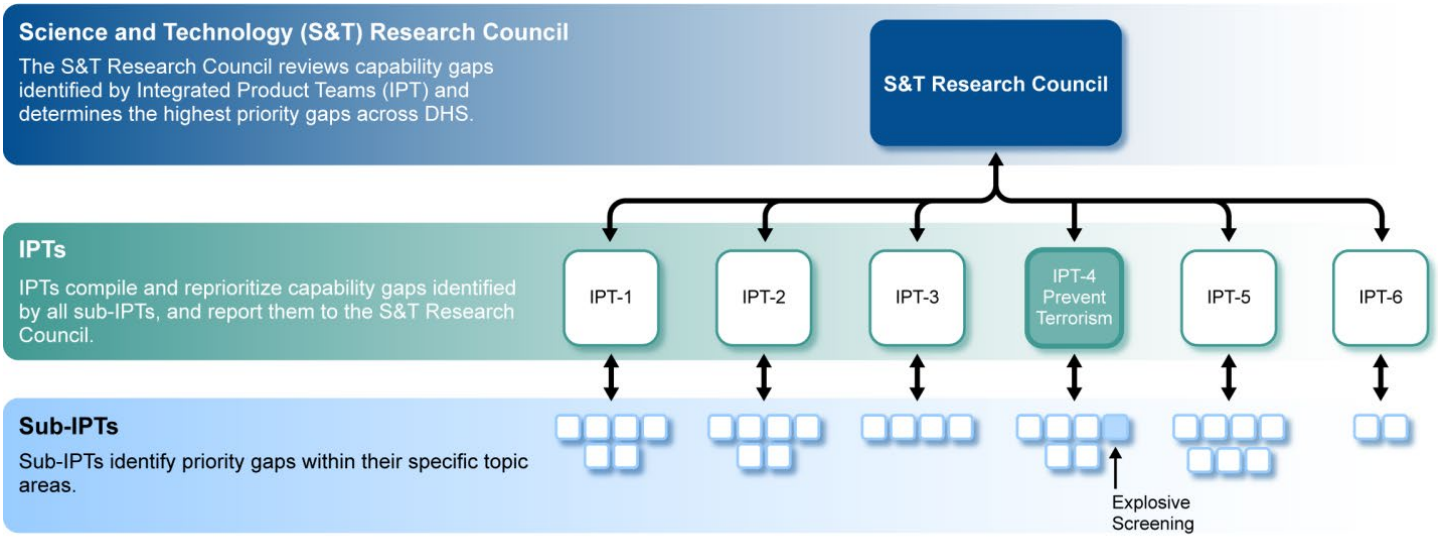
[15]See Exec. Order No. 13,416, 71 Fed. Reg. 71,033 (Dec. 7, 2006).

[16]The DHS IPT process was established in August 2015.

[17]As of October 2018, there are six IPTs and numerous supporting sub-IPTs, organized according to the Department's identified missions.

[18]We discuss the DHS IPT process for identifying mass transit security gaps later in the report.

Figure 2: Identification and Prioritization of Capability Gaps in the Department of Homeland Security (DHS) Research and Development Process



Source: GAO analysis of Department of Homeland Security (DHS) documents. | GAO-19-636

Note: The Prevent Terrorism IPT's Explosive Screening sub-IPT is responsible for identifying capability gaps relevant to surface transportation.

S&T. Once capability gaps are agreed upon and prioritized by DHS components through the IPT process, S&T undertakes R&D projects intended to address the highest prioritized capability gaps.[19] S&T can undertake R&D projects on behalf of any of the department's components, including TSA, and will either initiate development of a new technology solution or coordinate or adapt existing technologies to meet the project's needs.

Once S&T's R&D efforts result in a preliminary technology, or prototype, S&T will begin the testing process. S&T's technology development process includes developmental and operational testing phases that are carried out by staff at laboratories S&T contracts with. Developmental testing is typically conducted in simulated environments, such as laboratories, test facilities, or engineering centers, which can sometimes be representative of the complex operational environment (i.e., an actual subway station). Operational testing includes field tests performed under

[19]As the primary component for conducting R&D in the department, S&T's R&D portfolio includes projects designed to address a variety of capability gaps, such as land and sea cargo screening, biological threat detection, and port resiliency.

realistic conditions by actual users (i.e., the transit operators testing in a subway or rail station) and overseen by S&T in order to determine the effectiveness and suitability of a prototype technology. Once testing is complete, S&T contracts with staff at partner laboratories and works with private sector industry partners on further developing the product for the commercial market, where it can be purchased by mass transit operators to help secure their systems.

TSA. While TSA does not conduct R&D for mass transit security, it does sponsor testing of commercially available security technologies for the mass transit environment. This testing can take place in both laboratory environments and in operational, real-world environments. Regarding the latter, TSA uses its Surface Transportation Operational Test Bed Program (Operational Test Bed Program) to place commercially available security technologies in surface transportation environments, such as mass transit systems, for performance testing and evaluation.[20] TSA established the program to assess the effectiveness of emerging and existing security technologies in real-world environments; verify prior laboratory testing performance results versus performance in a TSA mass transit system (or other surface transportation mode serving as a test bed); and develop recommendations for use of certain technologies in surface transportation. As part of the program, TSA establishes memorandums of agreement with surface transportation entities that participate in the program and also provides them with logistical support, such as installing technology and providing personnel to help operators with technology training and operating needs. As of 2019, there are nine mass transit operators participating as test beds in the program (test beds), and TSA officials reported working to add two more mass transit agencies as test

[20]TSA started its test bed program in 2008 in response to the provision in the Implementing Recommendations of the 9/11 Commission Act requiring the establishment of a public transportation research and development program. Pub. L. No. 110–53, § 1409, 121 Stat. 266, 411 (2007) (codified at 6 U.S.C. § 1138).

beds.[21] In addition, there are five other surface transportation test beds, including two pipeline and two freight rail test beds.[22]

Mass Transit Operators. Mass transit operators generally do not have dedicated portions of their budgets for, and therefore do not conduct, R&D. However, selected operators work with TSA to test commercially developed technology solutions intended to enhance their system security. In general, mass transit operators must assume security-related expenses for their systems, including the purchase or acquisition of surface security technologies.[23]

S&T Has One Surface Transportation R&D Program Under Way, but Is Not Following DHS Guidance to Track Its Progress

[21]As of June 2019, TSA currently has memorandums of agreement with nine mass transit stakeholders for its Operational Test Bed Program: Amtrak, Bay Area Rapid Transit; Los Angeles Metro; Chicago METRA; New Jersey Transit; New York Police Department; Port Authority of New York and New Jersey; New York Metropolitan Transportation Authority; and Washington Metropolitan Area Transit Authority. TSA also has memorandums of agreement pending with Metropolitan Atlanta Rapid Transit Authority and Metrolink (commuter rail service in Southern California).

[22]The fifth test bed does not focus on a specific surface transportation mode, but tests technologies designed to protect critical infrastructure.

[23]The federal government has established grant programs to assist transit operators with these expenses.

S&T Is Developing Technologies to Address Explosive Threats within Mass Transit Stations

In 2010, S&T's Explosives Division began work on the Surface Transportation Explosive Threat Detection (STETD) program to address the threat of improvised explosive devices (IED) on persons or in objects within a mass transit station.[24] S&T officials stated that, as of fiscal year 2019, the STETD program remains S&T's sole R&D program related to surface transportation. In addition, it is the only DHS technology development program focused on developing products to address the threat of IEDs in a mass transit security environment.[25]

The STETD program consists of four separate technologies designed to address explosive threats within a mass transit station, each of which is in a different stage of development and maturation.[26] Specifically, the four technologies are known as Forensic Video Exploitation and Analysis (FOVEA), Standoff Detection, Real-Time Threat Detection Agent, and Layered Architecture. The technologies are designed to address unique aspects of the mass transit environment (i.e., multiple access points, lack of access barriers, etc.) while also working together to provide IED detection coverage from the point at which the passenger enters a mass transit station, boards a train, and then finally exits the system. These technologies would allow mass transit operators to scan large unstructured crowds to detect concealed explosives worn or carried on a person (person-borne IED), or placed in stationary objects such as

[24]An IED is a device fabricated in an improvised manner that incorporates in its designs explosives or destructive, lethal, noxious, pyrotechnic, or incendiary chemicals. S&T began this effort in 2010 with research into stakeholder requirements to address the threat of IEDs on persons or in objects within a mass transit station; the program was formally started once S&T concluded its research.

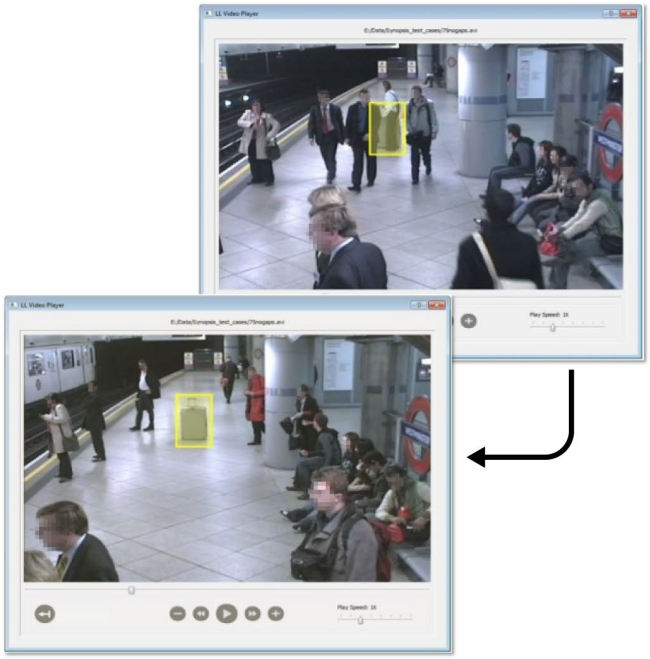
[25]The program's focus on various IED threats was derived from an analysis of existing mass transit security challenges, provisions in the Implementing Recommendations of the 9/11 Commission Act of 2007, formal requests made by TSA for the development of person-borne IED detection technologies, and feedback from mass transit stakeholders and the DHS IPT process. Specifically, S&T officials told us the STETD program is intended to meet the requirement that DHS establish a public transportation research and development program. The provision authorizes the use of funds to research chemical, biological, radiological, or explosive detection systems that do not significantly impede passenger access. Pub. L. No. 110–53, § 1409, 121 Stat. 266, 411 (2007) (codified at 6 U.S.C. § 1138). In addition, in 2013, TSA formally requested that S&T establish a program focused on researching and developing person-borne IED detection equipment, citing mass transit operators' feedback regarding their ability to conduct non-intrusive IED screening without impeding passenger flows within mass transit environments.

[26]According to S&T documentation, in addition to the mass transit environment, the four technologies being developed through the STETD program can also be used to monitor events that take place at stadiums, convention centers, or schools, as well as generally enhance security in any soft-target venue or environment with unstructured crowds.

	baggage, or intentionally deposited in an unnoticed location for detonation by a timer or remote control (leave-behind IED). S&T intends for STETD technologies to perform without requiring checkpoint baggage screening or other measures that could impede the traveling public moving through mass transit systems during periods of high passenger volume (e.g., rush hour).
FOVEA	FOVEA is a software suite designed to interface with video management systems already installed in mass transit systems, and is intended to help operators use recently recorded camera footage to quickly determine a person's movement through the system. S&T began developing the technology in fiscal year 2013, and it is generally directed at helping operators identify responsible parties when objects are left behind in a mass transit system. Specifically, FOVEA includes a number of tools to enable its video analysis (see figure 3).

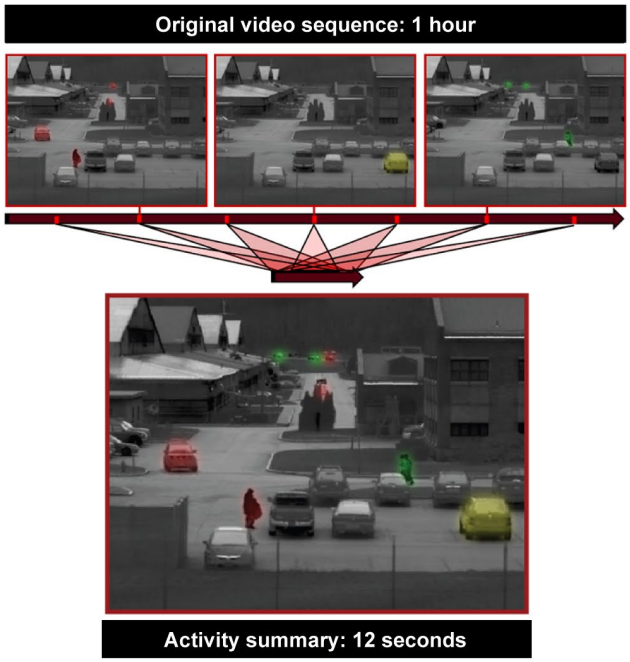
Figure 3: Forensic Video Exploitation and Analysis Tool Capabilities

Fast Event Review



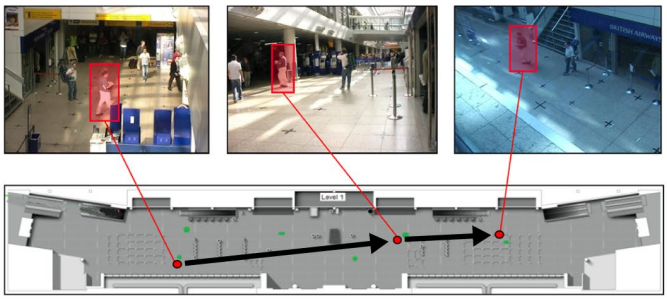
Gives users the ability to select an object within camera view and rapidly rewind the archived video to the point in time when a person or object first arrived. This allows an operator to review the circumstances surrounding the arrival (who, when, etc.).

Video Summarization



Transforms long durations of archived video into discrete activities in front of the camera (such as the path of a single passenger). This can be an effective way to reduce hours of video into a shorter timeframe when the user is seeking to identify a specific or anomalous activity taking place at an unknown time and position.

Path Reconstruction



Allows the user to mark within archived video the path an individual has traversed through the transit system. The capability allows an operator to follow a person across multiple cameras.

Source: GAO analysis of Department of Homeland Security Science and Technology Directorate documents. | GAO-19-636

As of December 2018, the FOVEA video suite has been installed in the Washington Metropolitan Area Transit Authority's Security Operations Control Center. During our site visit to the control center to view the use of the FOVEA suite, officials told us that FOVEA has enhanced the ability of personnel to analyze video footage for active law enforcement investigations. Officials also told us that because of this functionality, FOVEA is a valuable tool. S&T anticipates it will transition the technology to commercial development in fiscal year 2020.

Standoff Detection

S&T is developing a set of imaging sensors designed to scan unstructured crowds to detect hidden potential threat items (e.g., a person-borne IED) on travelers without requiring passengers to open bags or remove outerwear. According to S&T, the sensor technology would be placed in walls, near platforms, or other structures.[27] These screening devices are designed to unobtrusively scan for detailed information on possible person-borne threat objects, such as wires connected to a pressure cooker, and provide alerts to operators via the Real-Time Threat Detection Agent (described below). Development of these sensors began in fiscal year 2014, and since 2017, S&T officials have been using the Massachusetts Bay Transportation Authority training facility to test prototypes of the technology.[28] S&T expects to transition the technology to commercial development in fiscal year 2023.

Standoff Detection

Source: Department of Homeland Security Science and Technology Directorate. | GAO-19-636

[27]Standoff detection technologies can include active millimeter or centimeter wave frequencies, or terahertz frequencies, which are nonionizing radio waves that are part of the radio spectrum. Radiation in these waves are naturally emitted or reflected from everyday objects, including the human body, and has the added feature that clothing is often transparent to it. Therefore, these technologies can be used to safely screen people for hidden threat objects without impeding the flow of passengers.

[28]S&T officials selected this facility due to its capability to serve as a simulated operational environment. The Massachusetts Bay Transportation Authority is not a part of TSA's Operational Test Bed Program.

Real-Time Threat Detection Agent

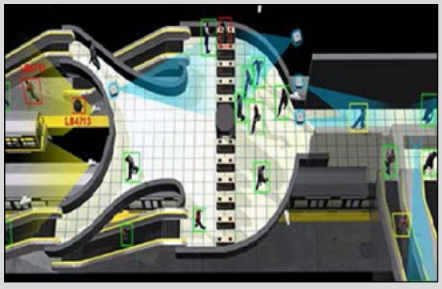
Real-Time Threat Detection Agent

Source: Department of Homeland Security Science and Technology Directorate. | GAO-19-636

The Real-Time Threat Detection Agent technology is intended to automatically detect abandoned objects that could be potential threats, and notify transit operators of their existence. Specifically, the system is to analyze live video footage to identify, tag (i.e., mark on the video footage), and track left-behind objects (i.e., baggage possibly containing IEDs), as well as individuals associated with the object, without the need for continuous human monitoring of video footage. To track potential IEDs without human monitoring, the system is intended to have the capability to identify abandoned objects that could be potential threats and compare them against defined criteria for person-borne, as well as leave-behind, IED threats.[29] Based on its analysis, the system would then create alerts and send them to operators, as well as to video review software, such as FOVEA. Development of this system began in fiscal year 2013, and S&T began developmental testing of the technology at Washington Metropolitan Area Transit Authority facilities in October 2018. S&T expects to transition the equipment to commercial development in fiscal year 2021.

Layered Architecture

Layered Architecture



Source: Department of Homeland Security Science and Technology Directorate. | GAO-19-636

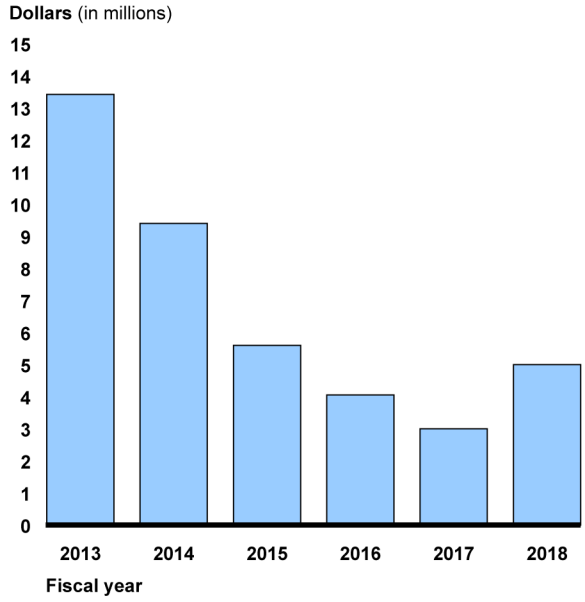
Layered architecture, the final component of the STETD program, is intended to have the capability to integrate information from the various existing security technologies utilized by a mass transit system to enable more accurate threat identification. The goal of this component is to gather input from multiple pieces of technology, such as distributed sensors and tools used across a mass transit environment (to include existing sensors and other STETD technologies), to present a consolidated threat profile to operators in a command center. This technological component is the least developed of the STETD program technologies, with ongoing work focused on experimentation with different prototypes. S&T expects to transition the technology to commercial development in fiscal year 2023.

[29]The technology is intended to utilize well-defined procedures and instructions used by computers to solve problems (i.e., algorithms) and machine learning to identify potential threat items.

STETD Program Funding

Since 2013, S&T's funding for mass transit R&D has decreased, delaying the development of associated technologies. Specifically, during fiscal years 2013 through 2017 funding for the STETD program—the only DHS R&D program focused solely on mass transit security—decreased by 78 percent, but then increased again in fiscal year 2018 (see figure 4).

Figure 4: DHS S&T Surface Transportation Explosive Threat Detection Program Budget for Fiscal Years 2013 through 2018



Source: GAO analysis of Department of Homeland Security (DHS) Science and Technology Directorate (S&T) program documents. | GAO-19-636

According to S&T officials, one reason funding was reduced during this period was to direct additional funds to R&D for a newly-identified threat. Specifically, in fiscal years 2015 and 2016, following the landing of a gyrocopter on the U.S. Capitol grounds and other incidents, unmanned aerial systems became a significant and emerging threat, and a top DHS priority. At the time, S&T had no funding allocated for a related R&D effort, so S&T leadership subsequently redirected funding from the STETD program toward R&D on unmanned aerial systems.

S&T officials told us that, due to fluctuations in funding, in addition to other factors, the program's completion date has shifted from 2017 to 2023, which has delayed efforts to make the technologies commercially available to mass transit operators. Although S&T began increasing funds for the STETD effort in 2018, according to program officials, decreases in

program funding have delayed program deliverables and pushed timelines out. For example, according to S&T officials, lower levels of program funding have made it difficult to employ highly-skilled contract staff at the laboratories S&T partners with to carry out STETD R&D, which has slowed the pace of development.[30] S&T officials also stated that a lack of funding and changes in funding slow down what is already a technically challenging development effort. As S&T officials explained, the STETD program is pushing the performance boundaries and capabilities of existing technologies, and in some cases, inventing entirely new technologies for screening highly trafficked environments.

S&T Has Not Developed Milestones to Effectively Track the Program's Progress

S&T is not using milestones that fully adhere to DHS guidance for milestone descriptions to track its progress on developing STETD technologies. Specifically, DHS budget development guidance directs DHS components to develop program milestones that are specific, measurable, results-oriented and relevant, and time-bound.[31] To be results-oriented and relevant, milestones must clearly link to activities in program strategy, budget, or other planning documents. Linking milestones to such activities allows parties reviewing the milestones, such as DHS leadership and Congress, to understand how achieving the milestones move the development process forward overall.

We assessed all 22 STETD milestones that S&T has used to report progress on the program from fiscal years 2013 through fiscal year 2018. We found that 17 of the 22 milestones were not results-oriented as required by DHS guidance because they did not clearly link to any key activities described by STETD program documents. Specifically, one STETD program document identified several key activities for completing

[30]S&T has contracted with the Massachusetts Institute of Technology's Lincoln Laboratory and Johns Hopkins University's Applied Physics Laboratory to carry out R&D work for the STETD program.

[31]DHS, *DHS Budget Build Framework*. (Washington, D.C.: Revised November 14, 2017). According to the guidance, milestones should be specific, measurable, attainable, results-oriented and time-bound. Milestones are specific when they provide a clear understanding of expected of results; attainable when they reflect a realistic plan of what may be accomplished within the fiscal year and with potential resources; measurable when they can be reported in quantitative or qualitative terms; and time-bound when they specify a beginning and end date for completion. According to our analysis, STETD milestones were specific, measurable, and time-bound. We did not assess S&T's STETD milestones against the criterion that they be attainable because we had no point of reference to determine whether milestones were realistic, given that the program was developing new technologies and capabilities.

work on the technologies, including a requirements development phase, developmental testing, and operational testing, but STETD milestones did not clearly link to these activities. For example,

- One fiscal year 2018 STETD milestone for the layered architecture technology was to conduct a simulation and analysis of layered sensing configurations to optimize sensor placement and system performance, to be completed by the end of fiscal year 2018. While this milestone was specific, measurable, and time-bound, it did not clearly link to a key activity (e.g., developmental or operational testing) identified in the STETD program's plan, and thus was not results-oriented.
- Another milestone from 2013 was to demonstrate advanced leave-behind detection software in a mass transit system. The milestone was to be met by the second quarter of fiscal year 2014, and remained unmet as of March 2019. Because the milestone was not results-oriented (i.e., it did not link back to activities in program documents), it was unclear how failing to achieve the milestone impacted, or potentially delayed, the overall technology development process.

S&T officials explained because they are dealing with technology innovation and invention, they plan to develop milestones that closely align to program plans after they develop a potential technology solution that is ready for developmental or operational testing. However, according to STETD program plans, it can take several years for STETD technologies to begin developmental testing. For example, one STETD technology (layered architecture) is not expected to begin developmental testing until the fiscal year 2021-2022 time frame. Therefore, under S&T's current practice, the program would not begin using results-oriented milestones, clearly linked to program plans, for this STETD technology until more than ten years after work on the program was initiated. Furthermore, we found that for one STETD technology (FOVEA), the program did not consistently use results-oriented milestones after the technology began developmental testing. Specifically, in fiscal year 2015 S&T began developmental testing for FOVEA, but, two of three FOVEA milestones reported in fiscal years 2017 and 2018 were not results-oriented.

Without milestones for the STETD program that reflect DHS guidance to clearly link the milestone to key events in program planning documents, Congress and DHS decision makers cannot fully assess whether the STETD program is meeting its goals within identified time frames.

Additionally, DHS decision makers are not positioned to identify adjustments that may be needed to facilitate the achievement of program goals.

We previously recommended in March 2019 that S&T take steps to more fully incorporate DHS's budget development guidance, to include more results-oriented milestones, for its R&D programs.[32] DHS concurred with this broader recommendation, and as of June 2019, is taking initial steps to ensure its implementation.

TSA Prioritizes Tests of Technology Products, but Projected Funding Shortfalls May Reduce the Scope of Future Testing

TSA Prioritizes the Testing of Technology Products to Secure Mass Transit Systems through Its Operational Test Bed Program

TSA sponsors tests of commercial products at contracted partner laboratories, as well as at mass transit stations and other surface transportation venues through its Operational Test Bed Program. The purpose of these tests is to inform surface transportation operators about different technological products that could address their security needs and to confirm whether the products will operate effectively.[33] As part of the testing process, TSA officials assist in product installation, hold technical demonstrations, and provide training for mass transit officials. Once product testing concludes, TSA officials document test results in written assessments, which they make available to mass transit and other surface transportation stakeholders to review upon request.

[32] Specifically, we recommended that S&T take steps to more fully incorporate leading practices, such as those included in DHS's budget preparation guidance, into R&D milestones. See GAO-19-210.

[33]TSA partner laboratories include Johns Hopkins University's Applied Physics Laboratory, the Naval Surface Warfare Center–Panama City Division, Raytheon, and Argonne National Laboratory.

TSA officials told us they use a number of methods to identify products that are currently available in the commercial marketplace and could be tested. Officials stated they conduct market research on vendors currently making technology products that could potentially meet the needs of mass transit operators, such as portable screening devices used to detect potential person-borne IEDs. To do so, officials maintain and utilize an existing list of vendors, conduct market research on their products, attend relevant symposiums and university conferences on technological advancements, and solicit information on these products and their capabilities from both vendors and operators who have used them. TSA officials also work with national laboratories to assist with relevant research on specific technological products and their capabilities that could be good candidates for testing.[34]

To determine which technology products to test, TSA prioritizes technologies that can be used in the mass transit environment. TSA officials told us that because of the level of risk facing mass transit systems, they generally try to ensure that the commercial products that are tested address capability gaps relevant to the mass transit environment.[35] In addition, TSA officials stated that while they try to address all identified surface transportation capability gaps, due to limited resources, they tend to select, on an annual basis, products for testing related to the following gaps: anomaly and explosive detection, high throughput threat detection, intrusion detection, infrastructure protection, and chemical and biological threat security, all of which have applicability to the mass transit environment.[36] Moreover, TSA officials told us that anomaly and explosive detection and high throughput threat detection are the technology gaps that are critical to securing mass transit systems.[37]

[34]These labs are the Massachusetts Institute of Technology's Lincoln Laboratory and Johns Hopkins University's Applied Physics Laboratory.

[35]TSA issues annually its Transportation Sector Security Risk Assessment—a report on transportation security that assesses risk by establishing risk scores for various attack scenarios within different transportation sectors, including surface transportation.

[36]As of 2019, unmanned aerial systems (i.e., drones) and remote area detection were two new gaps added to the list of existing surface transportation gaps to be addressed. Additionally, as of 2019, TSA and other stakeholders have identified 13 different capability gaps that exist across all modes of surface transportation (including mass transit) which should be addressed.

[37]High throughput threat detection refers to security measures designed to conduct non-intrusive or standoff screening of passengers, baggage, freight, and vehicles in areas where is a high concentration of available persons or objects to scan, such as large unstructured crowds or ticketing areas.

TSA officials also identify other criteria used for testing, including performance requirements and vendor claims about their products' ability to address specific capability gaps.

Regarding performance requirements, TSA officials told us any products selected for testing must meet a set of minimum performance requirements in order to be considered appropriate for addressing the unique security needs for different surface transportation modalities.[38] For example, for an explosive screening product used in mass transit, TSA officials established requirements for probability of detection and probability of false alarm. TSA officials stated they work with mass transit operators and others to identify these requirements to ensure that IED detection technologies can effectively identify threats without disrupting mass transit operations. Lastly, TSA officials said they also try to select technologies that can be used to secure multiple surface transportation modes. For example, officials said they may select an intrusion detection sensor for testing that could be adapted for securing pipelines or freight rail yards.

[38]With respect to mass transit test beds, TSA officials first contract with engineers from Johns Hopkins University's Applied Physics Laboratory and the Massachusetts Institute of Technology's Lincoln Laboratory to conduct preliminary assessments of certain products in their respective labs. Based on the results of these lab tests and the general performance requirements of mass transit operators, TSA officials then select specific products for operational testing and work with selected mass transit test beds to incorporate those products into their existing security processes.

TSA Tested Approximately 110 Existing Technology Products to Secure Surface Transportation Systems from Fiscal Years 2013 through 2018, but May Have to Reduce the Scope of Future Testing

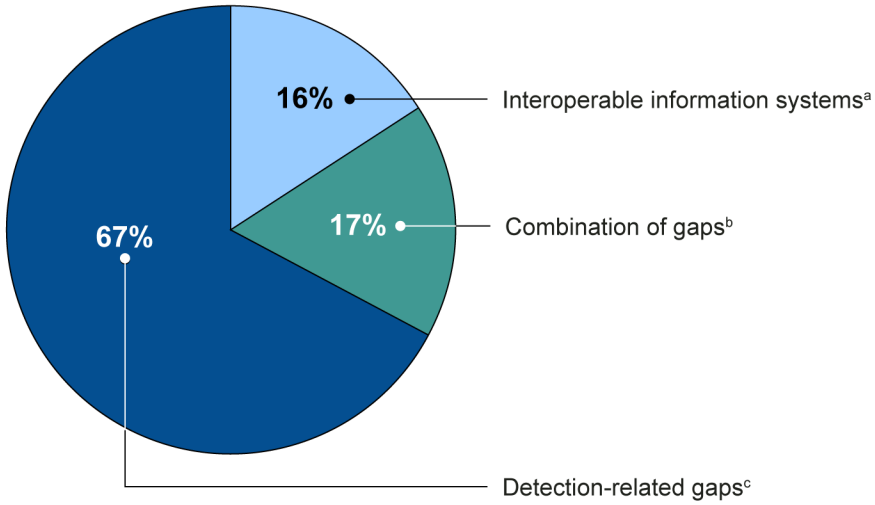
From fiscal years 2013 through 2018, TSA sponsored laboratory and field tests of approximately 110 commercial products that are designed to address identified surface transportation capability gaps (such as intrusion detection and explosive detection). These tests take place in either of two environments—laboratory or field (i.e., within a mass transit venue)—and are designed to address surface transportation security capability gaps.[39] Since 2013, 67 percent of the technology products (72 products) assessed by TSA focused on detection-related gaps, most of which were related to intrusion detection.[40] The remainder of products tested addressed interoperable information systems or a combination of capability gaps, such as anomaly and explosive detection and chemical and biological threat security (see figure 5).[41]

[39]TSA does not use its own laboratories to conduct any research or evaluation of commercial products. Instead, TSA uses its budget to leverage research of other entities, such as Johns Hopkins University's Applied Physics Lab.

[40]Intrusion detection sensors are physical security measures that are typically employed to detect unauthorized attempts to gain entry to, or suspicious activity near, a protected facility or asset. Most intrusion detection sensors are designed to work without being attended to by human guards (i.e., unattended) and in concert with other physical security measures, including barriers (e.g., fences), access control systems, camera surveillance systems, and video analytics software. Interoperable information system refers to products or tools that can be utilized by different types of information management systems available to operators. For example, a type of interoperable information system is a video footage analysis tool that can be integrated with different video management systems used by mass transit operators to record and store camera surveillance footage.

[41]Chemical and biological threat security refers to products or tools that can be utilized to prevent, respond to, or mitigate the effects of chemical or biological attacks. Examples of such products include those designed to identify or characterize a specific chemical or biologically-based threat compound (such as anthrax), as well as assist in decontamination of infrastructure, such as transit stations or tunnels. Interoperable information system refers to products or tools that can be utilized by different types of information management systems available to operators. For example, a video footage analysis tool that can be integrated with different video management systems used by mass transit operators to record and store camera surveillance footage.

Figure 5: Surface Transportation Capability Gaps Addressed by TSA Testing of Commercial Products, Fiscal Years 2013–2018 n=108



Source: GAO analysis of Transportation Security Administration (TSA) program documents. | GAO-19-636

[a]Interoperable information systems are products or tools that can be utilized by different types of information management systems available to operators. An example of such a system is a video footage analysis tool that can be integrated with different video management systems used by mass transit operators to record and store camera surveillance footage.

[b]Combination of gaps refers to technological products that TSA identified as applicable to more than one capability gap. An example is a screening device that could be used for anomaly and explosive detection as well as high throughput threat detection.

[c]Detection-related gaps refer to capability gaps which address the detection and identification of threats to the surface transportation environment, such as people, vehicles, and infrastructure. These gaps consist of anomaly and explosive detection, high throughput threat detection, chemical and biological threat security, and intrusion detection. High throughput threat detection refers to security measures designed to conduct non-intrusive or standoff screening of passengers, baggage, freight, and vehicles in areas where is a high concentration of available persons or objects to scan, such as large unstructured crowds or ticketing areas. Chemical and biological threat security refers to products or tools that can be utilized to prevent, respond to, or mitigate the effects of chemical or biological attacks. Examples of such products include those designed to identify or characterize a specific chemical or biologically-based threat compound (such as anthrax), as well as assist in decontamination of infrastructure, such as transit stations or tunnels. Intrusion detection sensors refer to physical security measures that are typically employed to detect unauthorized attempts to gain entry to, or suspicious activity near, a protected facility or asset. Most intrusion detection sensors are designed to work without being attended to by human guards (i.e., unattended) and in concert with other physical security measures, including barriers (e.g., fences), access control systems, camera surveillance systems, and video analytics software. The percentage of products tested for each of these capability gaps is sensitive security information and cannot be discussed in a publicly issued report.

Of the products that addressed more than one capability gap, 78 percent (14 of 18) of these products could be used for anomaly and explosive detection, as well as high throughput threat detection. TSA officials told us that because anomaly and explosive detection and high throughput threat detection technologies can be easily transported to different

locations within a station, they are of particular interest to mass transit operators.

On our site visits to two mass transit operators that TSA utilizes to test technology products, we observed the testing and use of commercial products.[42] These products were designed to detect anomalies on the underside of railcars as well as among persons traversing transit platforms, terminals, and stations. The products were being used to support both normal operations and a national security special event (see figure 6).[43]

Figure 6: Standoff Detection Technologies Being Tested in a Mass Transit System

Both the Qinetic SPO-NX (left) and ThruVision TAC (middle) technologies were used to scan passengers for anomalies and explosives (right).

Source: GAO. | GAO-19-636

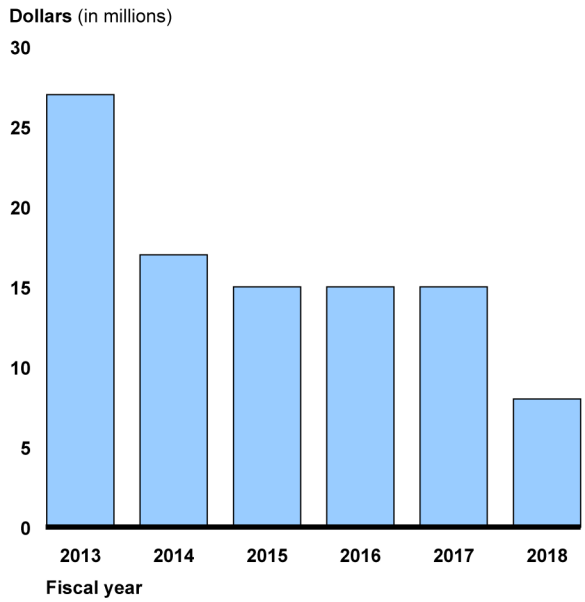
[42]One of these mass transit operators currently participates in TSA's Operational Test Bed Program; the other is working with TSA to become a test bed but has not yet signed a memorandum of agreement.

[43]One of these products had also been tested by one of TSA's partner laboratories before being deployed in mass transit test beds for testing. The other product had previously undergone TSA-led operational testing at a mass transit test bed to evaluate its capabilities.

Mass transit officials told us during our site visits that they considered these commercial technologies to be useful additions to their existing security measures. They also said the test results, which TSA made available to them, were helpful in determining whether to invest in purchasing the products for long-term use. In addition to allowing TSA to perform technology assessments, the program also gives transit operators hands-on experience with technologies they are unfamiliar with. For example, an official from one mass transit test bed told us that equipment often performs differently when the manufacturer's employees are operating it due to their prior experience with, and dedicated training on, the equipment. This official noted that transit system employees, who often do not have similar experience and training with a particular technology, can sometimes have different performance results when operating this equipment. The official told us that TSA's Operational Test Bed Program gives transit employees an opportunity to develop structured, hands-on experience with certain products with TSA's assistance, allowing them to understand the full potential and capabilities of the technology. This official said that, in her case, observing fellow transit employees using a particular technology for several hours convinced her of the product's application in a real-world environment, and subsequently was an important factor in her decision to recommend its purchase for use by her transit agency.

Although mass transit operators we spoke with valued the Operational Test Bed Program, TSA has decreased funding for the program since fiscal year 2013. Specifically, our analysis of program funding showed that the program experienced an approximately 70 percent decrease in funding from fiscal years 2013 through 2018 (see figure 7).

Figure 7: Funding for TSA Surface Transportation Operational Test Bed Program for Fiscal Years 2013 through 2018



Source: GAO analysis of Transportation Security Administration (TSA) program documents. | GAO-19-636

TSA officials stated that recent decreases in program funding, coupled with projected funding shortfalls for the Operational Test Bed Program for 2019 through 2024, will limit the program's capacity to conduct testing and assessments of technologies. Specifically, the TSA program manager for the Operational Test Bed Program told us that the recent decreases in funding for the program to its current level will materially impact the operation of the program moving forward. Furthermore, a TSA May 2019 budget planning document shows that, to fully meet project requirements, the program will require approximately $20 million in additional funding for fiscal years 2019 through 2024. Should the program not receive this funding, TSA officials stated they would not be able to test as many products or address as many surface transportation capability gaps through the program. They also stated that the funding shortfalls would limit TSA's analysis of technology performance. Program managers are in the process of identifying additional funding requirements for the program through TSA's internal budget review process.

Mass Transit Stakeholders Effectively Collaborate to Identify Capability Gaps and Test Security Technologies, but TSA Does Not Comprehensively Share Technology Assessments

S&T, TSA, and Mass Transit Operators Have Effectively Collaborated to Identify Mass Transit Capability Gaps and Test Technology Solutions through Four Key Mechanisms

S&T, TSA, and mass transit operators regularly collaborate on issues related to identifying mass transit capability gaps and testing security technologies to address those gaps. During the course of our review, we identified four key mechanisms that S&T, TSA, and mass transit operators use to collaborate on mass transit security issues—the DHS IPT process's sub-IPT focusing on surface transportation capability gaps (including those pertaining to mass transit); the Intermodal Transportation Systems Research and Development Working Group (RDWG); TSA's Operational Test Bed Program; and the Transit Policing and Security Peer Advisory Group (PAG) (see table 1).

Table 1: Collaborative Mechanisms Used to Identify Capability Gaps, Test Security Technologies, and Share Information Applicable to Mass Transit Security

Name	Description
Prevent Terrorism sub-IPT on Explosive Screening	The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) and the Transportation Security Administration (TSA) use the Prevent Terrorism Integrated Product Team's (IPT) Explosive Screening sub-IPT to identify surface transportation (including mass transit) capability gaps. Both S&T and TSA are members of the Explosive Screening sub-IPT, which identifies and prioritizes research and development technology needs to address identified surface transportation security technology capability gaps, among other things. As members of this sub-IPT, they can advocate for identified surface transportation capability gaps to be reported up to the Prevent Terrorism IPT and ultimately to the S&T Research Council to receive research and development funding.
Intermodal Transportation Systems Research and Development Working Group	TSA established this group in 2009 as the primary mechanism for S&T and TSA to gather input from surface transportation (including mass transit) stakeholders on security technology capability gaps. As of 2019, the group has 89 members from federal departments and agencies; industry; surface transportation stakeholders (including mass transit operators and associations); and subject matter experts. TSA chairs the working group and S&T is a member.
Surface Transportation Operational Test Bed Program	TSA and S&T use the Surface Transportation Operational Test Bed Program to collaborate with mass transit operators to assess security technologies. As part of the program, TSA establishes memorandums of agreement with mass transit operators that facilitate its testing of commercially developed technologies.[a] In addition, S&T leverages these agreements to test technologies it is developing through its Surface Transportation Explosive Threat Detection Program.
Transit Policing and Security Peer Advisory Group	TSA established this group in 2007 as a communication and liaison group consisting of transit police chiefs and security directors from mass transit systems across North America. The group is designed to provide subject matter expertise on mass transit security-related issues. The group has 33 mass transit stakeholder members and is chaired by a transit police chief.

Source: GAO analysis of DHS program documents. | GAO-19-636

[a]As of June 2019, TSA currently has memorandums of agreement with nine mass transit stakeholders for its Surface Transportation Operational Test Bed Program: Amtrak; Bay Area Rapid Transit; Los Angeles Metro; Chicago METRA; New Jersey Transit; New York Police Department; Port Authority of New York and New Jersey; New York Metropolitan Transportation Authority; and Washington Metropolitan Area Transit Authority. TSA also has memorandums of agreement pending with Metropolitan Atlanta Rapid Transit Authority and Metrolink (commuter rail service in Southern California).

Leading Practices for Implementing Interagency Collaborative Mechanisms

Although collaborative mechanisms differ in complexity and scope, they all benefit from certain key features, including

- **Outcomes and Accountability:** Have short-term and long-term outcomes been clearly defined? Is there a way to track and monitor their progress?
- **Bridging Organizational Cultures**: What are the missions and organizational cultures of the participating agencies? Have agencies agreed on common terminology and definitions?
- **Leadership: How will leadership be sustained over the long-term?** If leadership is shared, have roles and responsibilities been clearly identified and agreed upon?
- **Clarity of Roles and Responsibilities:** Have participating agencies clarified roles and responsibilities?
- **Participants:** Have all relevant participants been included? Do they have the ability to commit resources for their agency?
- **Resources:** How will the collaborative mechanism be funded and staffed? Have online collaboration tools been developed?
- **Written Guidance and Agreements**: If appropriate, have participating agencies documented their agreement regarding how they will be collaborating? Have they developed ways to continually update and monitor these agreements?

Source: GAO, *Managing for Results: Key Considerations for Implementing Interagency Collaborative Mechanisms*, GAO-12-1022 (Washington, D.C.: Sept. 27, 2012). | GAO-19-636

We assessed the effectiveness of collaboration in these four mechanisms using our leading collaboration practices (see side bar) and found that each of them generally followed these practices.[44] We reported in March 2019 that DHS-wide R&D collaboration has improved through the IPT process but some challenges remain, such as ensuring all components participate in the process, among other things.[45] However, as discussed below, we found that S&T and TSA collaborate effectively through the IPT process for identifying mass transit security capability gaps and security technologies.

Prevent Terrorism sub-IPT on Explosive Screening. S&T and TSA collaborate on identifying surface transportation (including mass transit) capability gaps through the Prevent Terrorism's sub-IPT on Explosive Screening. At the federal level, we found that TSA and S&T's ongoing use of this mechanism met several leading collaboration practices, including bridging organizational cultures, leadership, clarity of roles and responsibilities, participants, and written guidance and agreements.[46] Specifically, the Explosive Screening sub-IPT has a formal structure that is outlined in the Prevent Terrorism IPT's charter. This written agreement establishes leadership and clarifies the roles and responsibilities of each of the participants. As key participants and voting members, S&T and TSA possess the necessary expertise to identify capability gaps for mass transit (i.e., S&T has expertise in technology research and development, and TSA has in-depth knowledge of the mass transit and other surface transportation sectors). Moreover, by requiring S&T and TSA to work together to prioritize capability gaps, the process allows them to operate across agency boundaries (i.e., to bridge their respective organizational structures). In 2012, S&T officials stated that they collaborated with TSA as members of the Explosive Screening sub-IPT to identify anomaly and explosive detection and high-throughput threat detection as the highest priority capability gaps for surface transportation. These gaps were the basis for S&T's STETD program.

[44]In cases where a collaboration practice did not apply to a mechanism, we did not assess the mechanism by the practice. For each collaborative mechanism, we indicate the practices we did not assess them by and why.

[45]See GAO-19-210.

[46]We did not assess whether S&T and TSA have clearly defined the outcomes, or whether progress has been tracked and monitored by the Explosive Screening sub-IPT, because final decisions and accountability for identifying gaps are performed by S&T Research Council and involve the DHS-wide IPT process, which is outside of the sub-IPT's authority.

RDWG. We also found that the RDWG facilitates effective collaboration between S&T, TSA, and surface transportation stakeholders, including 30 mass transit operators.[47] The RDWG generally follows leading collaboration practices related to bridging organizational cultures, leadership, clarity of roles and responsibilities, participants, resources, and written guidance and agreements.[48] Specifically, the RDWG is a working group with an established charter that brings together federal and surface transportation representatives to operate across agency and sector boundaries to identify surface transportation-related capability gaps, including those for mass transit. The RDWG charter clarifies the participant roles and responsibilities and establishes a framework for nominating new members to ensure all relevant participants are included. TSA, as the designated chair, funds the working group and ensures its continuation. In addition to identifying surface transportation security gaps, an S&T official told us that the members of the RDWG review the prior year's security capability gaps to determine whether they are still relevant and if there are commercially available technologies to address them. The S&T official explained that they then use the results of these reviews to inform their work on the Explosive Screening sub-IPT, specifically using them as basis for R&D project requirements. For example, S&T officials said that anomaly and explosive and high-throughput threat detection were the gaps identified by the participants of the RDWG and then reported through the DHS IPT process, which ultimately helped inform the scope of S&T's STETD program. In addition, S&T officials told us that they use the RDWG annual meetings to communicate to surface transportation stakeholders the progress they have made to address these gaps through the STETD program.

Operational Test Bed Program. TSA's Operational Test Bed Program facilitates collaboration between S&T, TSA, and mass transit operators on the testing and evaluation of security technologies. The program, through its memorandums of agreement with mass transit operators, generally follows leading collaboration practices related to collaboration criteria for bridging organizational cultures, clarity of roles and responsibilities,

[47]The RDWG's membership includes all surface transportation stakeholders and not just mass transit. In addition to the surface transportation and mass transit stakeholders, as of June 2019 the RDWG has 125 members from federal, state, local, and international agencies, industry, and subject matter experts.

[48]We did not asses the RDWG as a collaborative mechanism by the Outcomes and Accountability criterion because final decisions and accountability for identifying gaps out are performed by a different entity, the S&T Research Council.

participants, resources, and written guidance and agreements.[49] Specifically, memorandums of agreement serve as a mechanism for TSA and S&T to operate outside of their agency boundaries to test technologies in real-world environments (i.e., mass transit systems). The agreements also clarify the roles and responsibilities and serve as guidance for TSA, S&T, and mass transit operators on how testing is to be carried out. For example, the agreements clarify responsibilities for installing and operating test equipment. The program is funded and managed by TSA, and S&T and mass transit operators leverage TSA's resources through their participation. Collaboration through the program has led to numerous benefits for TSA, S&T, and mass transit operators. According to TSA officials, the program allows TSA to fulfill federal requirements to test and evaluate mass transit security technologies and to expand the market for these products.[50] Additionally, S&T has used the program's established agreements with transit systems to facilitate the testing of STETD program prototypes. Lastly, transit operators use the program to obtain first-hand information on the performance of security technologies within their system. For example, an official from one mass transit operator participating in the test bed program told us they purchased two different types of passive millimeter wave scanners that they tested through the program and found to be effective.

Transit Policing and Security Peer Advisory Group (PAG). The PAG facilitates collaboration among mass transit stakeholders to share information and meets the bridging organizational cultures, leadership, participants, resources, and written guidance and agreements

[49]We did not assess the Operational Test Bed Program's memorandums of agreement by the Outcomes and Accountability and Leadership key features because the memorandums do not address these activities.

[50]Executive Order 13416: *Strengthening Surface Transportation Security*, requires DHS to develop, implement, and lead a process to coordinate research, development, testing, and evaluation of technologies related to the protection of surface transportation. Exec. Order No. 13,416, 71 Fed. Reg. 71,033 (Dec. 7, 2006). Section 1409 of the Implementing Recommendations of the 9/11 Commission Act of 2007 requires DHS to carry out a research and development program for the purpose of improving the security of public transportation systems. As part of this program, funds may be used to conduct product evaluations and testing. See Pub. L. No. 110–53, § 1409, 121 Stat. 266, 411 (2007) (codified at 6 U.S.C. § 1138). As part of its testing and evaluation, TSA works with public and private sector partners to ensure technologies meet the evolving needs of security end-users, thereby expanding the marketplace for commercially developed products to support the enhancement of surface transportation security.

collaboration key features criteria.[51] Specifically, the PAG follows several practices through its charter, which designates a transit police chief as the chair of the group. The charter also outlines the participating mass transit stakeholders and allows them to share information across agency boundaries on security-related issues, including information on incident response, emerging threats, and other best practices on mitigating security issues. Officials from all nine of the mass transit operators we spoke with are members of the PAG, and seven of them stated that the PAG fosters collaboration between mass transit operators by providing a forum for transit officials to connect and share information. Particularly, one mass transit operator stated that the PAG was beneficial to the safety and security of her system because it has allowed mass transit officials to share experiences and disseminate best practices for responding to threats. Another official said that the PAG helped him stay informed about the current risks facing all of the mass transit operators, and without the group, collaboration probably would not happen.

TSA Engages in Collaborative Activities to Share Information on Security Technologies, but Does Not Comprehensively Share Technology Assessment Information

TSA engages in a number of collaborative activities to share information on security technologies with mass transit stakeholders to help improve their technology investments. Specifically, TSA disseminates a quarterly newsletter to surface transportation stakeholders (including mass transit operators) which summarizes TSA's efforts to address various surface transportation security issues. Among other things, the newsletter shares information on the technologies for which TSA has sponsored testing in different mass transit operator systems. Additionally, TSA maintains a collective email account that was created for all mass transit operators to send TSA suggestions for technologies or products to test, among other things. Further, TSA officials stated that they notify and communicate to regional mass transit stakeholders any information on upcoming test bed demonstrations, so these stakeholders can attend in person if they prefer. Finally, according to the TSA program manager, TSA officials utilize the American Public Transportation Association's annual conference, industry symposiums, and security roundtables to engage with mass transit

[51]We did not assess the PAG as a collaborative mechanism by the outcomes and accountability, clarity of roles and responsibilities, and resources key features because the group is used solely for the purpose of sharing information, and, therefore, there are no specified outcomes to be achieved or roles to be played beyond using the group to disseminate information. In addition, because the PAG collaborates through monthly and as needed conference calls, the PAG does not require any funding to sustain it.

stakeholders to share information on security threats, capability gaps, and technology.

In addition, to assist transit operators, TSA produces a number of assessments and reports (products) that include performance information on a range of technologies. These products include:

- **TSA's Market Survey**. TSA officials regularly update a market survey, which contains a list of commercial vendors who develop technological products capable of addressing surface transportation security issues. This list, which does not contain sensitive information and may be readily shared with operators, includes vendors and their associated products that TSA believes may be applicable to mass transit security; it does not catalog the list of products TSA has sponsored testing for. TSA officials populate this list by attending relevant symposiums and university conferences, as well as soliciting input from partner laboratories.
- **Surface Transportation Sensor Catalog**. The Surface Transportation Sensor Catalog documents the technology assessments performed by TSA and contains summaries of various security technologies evaluated since 2007. In addition to evaluated products, it also contains summaries of the vendor product demonstrations received by TSA since fiscal year 2016.[52] TSA officials stated that the catalog is updated each year with new entries for recently evaluated products, and is intended as a resource for both TSA and its stakeholders to have greater awareness of technologies and help them make more informed technology investment decisions.

[52]In general, the catalog highlights technologies applicable for surface transportation and public area security applications. This includes systems capable of detecting mass casualty threats (such as IEDs, bladed weapons, and firearms), trace quantities of explosives on outer surfaces, and unauthorized intruders. These reports contain sensitive information and cannot be distributed without assessing whether the requester is eligible to receive them.

- **State of Technology Reports**. TSA publishes a State of Technology report that provides a detailed overview of a specific challenge to surface transportation stakeholders (such as person-borne IEDs) and gives a high-level summary of available products that could address it, and a technology maturation roadmap (with objectives) that needs to be implemented in order to meet surface transportation stakeholders' operational and security needs to address those specific threats.[53]

Although these TSA products contain technology assessment and other information that would benefit mass transit operators seeking to purchase and implement security technologies, mass transit operators may not be receiving them. Specifically, TSA shares these products with transit operators upon request. However, officials from seven of the nine mass transit operators that we spoke with said they wanted more technical assessment information on commercially available security technologies, indicating that they may not be routinely requesting, and therefore not receiving, the TSA products that would provide this information. In addition, four of the nine said they would like TSA's assessment information on technologies to be more accessible. Finally, an official from one mass transit system who previously worked for TSA on mass transit issues, and thus has knowledge of the broader mass transit community, stated that many operators would benefit from the Surface Transportation Sensor Catalog, but smaller operators are not aware of this resource and therefore do not know how to request it.

TSA officials stated they do not routinely share information on security technologies with mass operators for two reasons. First, TSA officials explained that many of the in-depth reports that result from its testing of security technologies contain sensitive information and cannot be distributed without first assessing whether the requester is eligible to receive it. However, officials from most of the mass transit operators we spoke with said they would like more technical assessment information. Therefore it could be useful for mass transit operators to know when TSA publishes these reports so they can request the full report for review. This notification could consist of non-sensitive, high-level information on technologies assessed so that mass transit operators could request the information in full. Second, the TSA program manager responsible for these assessments told us that his office does not have sufficient resources to develop and maintain a centralized, web-based repository

[53]These reports contain sensitive information and cannot be distributed without assessing whether the requester is eligible to receive them.

that would allow mass transit operators to search and retrieve sensitive information independently, such as the sensor catalog and technology assessment reports.

Despite these limitations, in the past, TSA has shared information related to technology assessments routinely with mass transit operators. For example, TSA used to post a verified technology list on a Federal Emergency Management Agency web page. A TSA official stated that the information posted on the website included summary information on technology evaluations and other technology information. Further, TSA received feedback from surface transportation (including mass transit) stakeholders that the information posted was useful. TSA no longer posts information on the web page because the Federal Emergency Management Agency no longer maintains the website. In addition, TSA officials stated that they had plans to include more comprehensive information about TSA's technology assessments within an online information resource known as the DHS Responder Knowledge Base—a department-wide database previously developed to house information for first responders.[54] In April 2019 officials from DHS's Countering Weapons of Mass Destruction Directorate said they had plans to reach out to TSA and other DHS components on how to utilize the Responder Knowledge Base as a repository for their reports and other sensitive information.[55] Furthermore, officials from that directorate told us that the database is about 2 years from being launched, and they do not have a specific completion date.

Standards for Internal Control in the Federal Government states that management should communicate externally to their stakeholders through the appropriate means.[56] Further, the *2013 National*

[54]DHS developed the database in 2002 to serve as an online repository for first responders to access information on products, standards, certifications, grants, and other equipment-related information.

[55]TSA's goals for the updated Responder Knowledge Base include sharing timely information on test and evaluation results of surface security technologies and information on upcoming security technology pilots and demonstrations for surface transportation stakeholders. Additionally, TSA plans to use the knowledge base as another communication and outreach platform to create a forum for the surface transportation community to exchange information on upcoming events, opportunities, and best practices with their peers. According to DHS officials from the Countering Weapons of Mass Destruction Directorate, plans for the knowledge base would allow TSA to store sensitive information and reports on technologies.

[56]GAO-14-704G.

Infrastructure Protection Plan states that in order to ensure that situational awareness capabilities keep pace with the evolving risk environment, officials should improve practices for sharing information that will improve security and resilience.[57] Until the Responder Knowledge Base is operational, mass transit operators could benefit from TSA routinely sharing appropriate information on the technology assessments and other performance information at its disposal. For example, TSA could leverage the resources of existing coordination mechanisms, like the PAG, or develop a listserv to automatically notify a more comprehensive group of mass transit operators of the existence of a new technology assessment or sensor catalog. Notifying more mass transit operators on an ongoing basis that this information is available would help ensure they have the benefit of all relevant TSA information when making strategic security technology investments. Further, doing so would help mass transit operators to better use their limited resources to acquire proven technologies that could enhance the overall security posture of their systems.

Conclusions

Monitoring and securing surface transportation systems continues to present unique challenges. With respect to mass transit systems, for example, operators must balance the need to efficiently move passengers through the system with the need to screen for explosives and other threats. Since 2010, S&T's STETD program has been the only DHS R&D program that has developed technologies to address these challenges. Although S&T has made progress, as of fiscal year 2019, none of the technologies associated with the STETD program have matured enough to undergo commercial development, and the program's completion date has been extended from fiscal year 2017 to fiscal year 2023. While fluctuations in the program's funding have contributed to delays, S&T has not followed DHS guidance for developing milestones that would help officials understand whether the program is achieving key activities identified in planning documents when faced with funding and other challenges. Without milestones that clearly convey an understanding of the program's progress, DHS decision makers are not positioned to identify any adjustments that may be needed to facilitate the achievement of program goals.

[57] *National Infrastructure Protection Plan* 2013.

S&T, TSA, and mass transit operators effectively collaborate through a number of stakeholder groups to identify mass transit security gaps and to test possible technology solutions that could address them. TSA also supports greater awareness of available technologies by publishing key information on commercially available products (such as technology assessment results) and making it available to mass transit operators upon request. However, TSA does not comprehensively or routinely share this information, and seven of the nine mass transit operators we spoke with stated they wanted more technology assessment information. Without a mechanism to share technology assessments and related information with more mass transit operators and on a routine basis, TSA cannot ensure that mass transit operators will be fully informed about available technologies they could use to secure their systems. Moreover, without this information, mass transit operators may not be positioned to make the best possible use of the limited funding available for purchasing these technologies.

Recommendation for Executive Action

We are making two recommendations, one to DHS and one to TSA.

The Deputy Secretary of Homeland Security should ensure that S&T take steps to more fully incorporate practices for developing milestones within DHS's budget preparation guidance, into the Surface Transportation Explosive Threat Detection program. (Recommendation 1)

The Administrator of TSA should develop a mechanism to more routinely and comprehensively share appropriate information on the performance of mass transit security technologies (such as the annual sensor catalog and security technology assessments) with mass transit operators and stakeholders until DHS completes work on a more permanent information sharing resource. (Recommendation 2)

Agency Comments and Our Evaluation

We provided a draft of this report to S&T and TSA for review and comment. DHS provided written comments which are reprinted in appendix I. In its comments, DHS concurred with both recommendations and described actions planned to address them. S&T and TSA also provided technical comments, which we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees and the acting Secretary of Homeland Security. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff members have any questions about this report, please contact William Russell at (202) 512-8777 or russellw@gao.gov. Contact points for our Office of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix II.

W. William Russell
Acting Director,
Homeland Security and Justice

List of Requesters

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
House of Representatives

The Honorable John Katko
Ranking Member
Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation
Committee on Homeland Security
House of Representatives

The Honorable Michael T. McCaul
House of Representatives

The Honorable Bonnie Watson-Coleman
House of Representatives

Appendix I: Comments from the U.S. Department of Homeland Security

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

Homeland Security

September 3, 2019

W. William Russell
Acting Director, Homeland Security and Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management Response to Draft Report GAO-19-636, "SURFACE TRANSPORTATION: DHS Is Developing and Testing Technologies but Could Better Share Test Results"

Dear Mr. Russell:

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

The Department is pleased to note GAO's positive recognition that the Science and Technology Directorate (S&T), Transportation Security Administration (TSA), and mass transit operators effectively collaborate to identify mass transit security gaps and discuss possible technological solutions that could address them. The nature of threats facing the Nation's surface transportation networks are broad and ever evolving. DHS remains committed to working with its partners inside and outside of government to develop efficient, effective, real-world solutions that address security vulnerabilities.

The draft report contained two recommendations with which the Department concurs. Attached find our detailed response to each recommendation. Technical comments were previously provided under separate cover.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Attachment

Attachment: Management Response to Recommendations Contained in GAO-19-636

GAO recommended that the Deputy Secretary of Homeland Security:

Recommendation 1: Ensure that S&T take steps to more fully incorporate practices for developing milestones within DHS's budget preparation guidance, into the Surface Transportation Explosive Threat Detection program.

Response: Concur. S&T's Mission and Capability Support Office, Physical and Cyber Security Division, is currently preparing its input for DHS's FY 2021 Budget Justification. This justification will include linking milestones to key activities for research and development projects, such as those involving Surface Transportation Explosive Threat Detection technologies, that are far enough along in developmental and operational testing to provide meaningful information to facilitate the achievement of program goals. Estimated Completion Date (ECD): April 30, 2020.

GAO recommended that the Administrator of TSA:

Recommendation 2: Develop a mechanism to more routinely and comprehensively share appropriate information on the performance of mass transit security technologies (such as the annual sensor catalog and security technology assessments) with mass transit operators and stakeholders until DHS completes work on a more permanent information sharing resource.

Response: Concur. Until DHS deploys the Responder Knowledge Base as discussed in the draft report, TSA's Operations Support will:

- Expand the distribution of the Surface Transportation Sensor Catalog commensurate with security considerations, ensuring that the body of data and information provided cannot be aggregated by a recipient over time to create a collection of data that would otherwise be classified or labeled as Sensitive Security Information if provided by itself ("classification by aggregation"),
- Explore the feasibility of providing appropriate information on the performance of mass transit security technologies through the Homeland Security Information Network or similar platforms when new information becomes available, and
- Provide updates on the performance of mass transit security technologies in conjunction with scheduled Surface Transportation Security Advisory Committee meetings.

ECD: February 28, 2020.

2

Appendix II: GAO Contact and Staff Acknowledgments

GAO contact

William Russell (202) 512-8777 or RussellW@gao.gov.

Staff Acknowledgments

In addition to the contact named above, Christopher Ferencik (Assistant Director), Mona Nichols Blake (Analyst in Charge), Jason Blake, Frederick K. Childers, Michele Fejfar, Jonathan G. Felbinger, Eric Hauswirth, Tracey King, Kristiana D. Moore, Claire Peachey, Jack Sheehan, Sarah Veale, and Robert Ward made key contributions to this report.