



September 2017

AVIATION SECURITY

Actions Needed to Systematically Evaluate Cost and Effectiveness Across Security Countermeasures

Accessible Version

GAO Highlights

Highlights of [GAO-17-794](#), a report to congressional requesters

Why GAO Did This Study

Since the attacks of September 11, 2001, TSA has spent billions of dollars on aviation security programs. However, recent attacks involving aircraft and airports in other countries underscore the continued threat to aviation and the need for an effective aviation security program.

GAO was asked to review TSA's passenger aviation security countermeasures. This report examines the extent to which TSA has (1) information on the effectiveness of selected passenger aviation security countermeasures and (2) systematically analyzed the cost and effectiveness tradeoffs among countermeasures.

GAO reviewed TSA documentation on the effectiveness of six passenger aviation security countermeasures in fiscal year 2015—the most recent year for which data were available. GAO selected these countermeasures because they involve direct interaction with passengers, their belongings, or their personal information, and are largely operated and funded by TSA. GAO also reviewed TSA documents and interviewed TSA officials regarding efforts to systematically analyze cost and effectiveness tradeoffs across countermeasures.

What GAO Recommends

GAO recommends that TSA (1) explore and pursue methods to assess the deterrent effect of TSA's passenger aviation security countermeasures, with FAMS as a top priority to address, and (2) systematically evaluate the potential cost and effectiveness tradeoffs across aviation security countermeasures. DHS concurred with these recommendations.

View [GAO-17-794](#). For more information, contact Jennifer Grover at (202) 512-7141 or groverj@gao.gov.

September 2017

AVIATION SECURITY

Actions Needed to Systematically Evaluate Cost and Effectiveness Across Security Countermeasures

What GAO Found

The Transportation Security Administration (TSA) has data on the effectiveness of some, but not all of its passenger aviation security countermeasures. Specifically, TSA has data on passenger prescreening, checkpoint and checked baggage screening, and explosives detection canines. Further, TSA is taking steps to improve the quality of this information. However, it does not have effectiveness data for its Behavior Detection and Analysis (BDA) program and the U.S. Federal Air Marshal Service (FAMS). For BDA—a program to identify potential threats by observing passengers for behaviors indicative of stress, fear, or deception—in July 2017, GAO reported that (1) TSA does not have valid evidence supporting most of its behavioral indicators, and (2) TSA should continue to limit future funding for its behavior detection activities until it can provide such evidence. For FAMS—a program that deploys armed law enforcement officers on certain flights at an annual cost of about \$800 million for fiscal year 2015—officials reported that one of the primary security contributions is to deter attacks. However, TSA does not have information on its effectiveness in doing so, nor does it have data on the deterrent effect resulting from any of its other aviation security countermeasures. While officials stated that deterrence is difficult to measure, the Government Performance and Results Act of 1993, as updated, provides that agencies are to assess the effectiveness of their programs. Further, the Office of Management and Budget and GAO have suggested approaches for measuring deterrence. Developing such methods for TSA countermeasures, especially for an effort such as FAMS in which the primary goal is deterrence, would enable TSA to determine whether its substantial investment is yielding results.

TSA has a tool to compare the security effectiveness of some aviation security countermeasures, but has no efforts underway to systematically evaluate potential cost and effectiveness tradeoffs across all countermeasures. In 2014, the agency developed a tool to analyze the security effectiveness of alternate combinations of some countermeasures for the purpose of informing acquisition and deployment decisions, but does not have a tool to assess such tradeoffs across the entire system of countermeasures. TSA officials explained that the aviation security system is constantly evolving, and assessing a system in flux is challenging. However, DHS policy and TSA's strategic plan call for the systematic evaluation of costs and effectiveness of TSA's chosen mix of aviation security countermeasures. Without such an analysis, TSA is not well positioned to strike an appropriate balance of costs, effectiveness, and risk.

This is a public version of a classified report that GAO issued in August 2017. Information that TSA deemed classified or sensitive security information, such as the results of TSA's covert testing and details about TSA's screening procedures, have been omitted.

Contents

Letter	1
Background	4
TSA Has Effectiveness Data on Some Countermeasures That Show Mixed Results, But Does Not Measure Deterrence	13
TSA Can Compare the Effectiveness of Certain Combinations of Aviation Security Countermeasures, but Does Not Systematically Analyze Cost and Effectiveness Tradeoffs Across All Countermeasures	22
Conclusions	26
Recommendations for Executive Action	27
Agency Comments and Our Evaluation	27
Appendix I: Transportation Security Administration (TSA) Information on the Direct Costs of Selected Countermeasures	30
Appendix II: Fiscal Year 2015 Effectiveness Data for Selected Passenger Aviation Security Countermeasures	33
Appendix III: Comments from the Department of Homeland Security	57
Appendix IV: GAO Contact and Staff Acknowledgments	62
Appendix V: Accessible Data	63
Data Table	63
Agency Comment Letter	64

Tables

Table 1: Transportation Security Administration (TSA) Information about Selected Countermeasure Effectiveness in Detecting and Disrupting Threats to Aviation Security in Fiscal Year 2015	17
Table 2: Direct Cost of Selected Transportation Security Administration (TSA) Passenger Aviation Security Countermeasures in Fiscal Year 2015	31

Table 3: Summary of Transportation Security Administration (TSA) Checkpoint Screening Technologies Deployed in Fiscal Year 2015	40
Table 4: Description of Annual Proficiency Review (APR) Component Tests for Checkpoint Screening in Calendar Year 2015	42
Table 5: Description of Annual Proficiency Review (APR) Component Tests for Checked Baggage Screening in Calendar Year 2015	51
Table 6: Total Number, Roles, and Responsibilities of Transportation Security Administration (TSA) Canine Teams by Type of Team Deployed in the Aviation Environment as of September 2015	54

Figures

Figure 1: Illustrative Example of a Passenger Experience with Selected Transportation Security Administration (TSA) Countermeasures	6
Figure 2: Examples of Aviation Security Countermeasures Deployed or Expanded, 2001-2017	12
Figure 3: Transportation Security Administration (TSA) Passenger Prescreening Process	35
Figure 4: Transportation Security Administration's (TSA) Passenger Screening Checkpoint	39
Figure 5: A Checked Baggage Inspection Configuration That Includes Three Explosives Detection Systems	49
Figure 6: Transportation Security Administration (TSA) Canine Team Searches an Airport Terminal	54
Accessible Data for Figure 2: Examples of Aviation Security Countermeasures Deployed or Expanded, 2001-2017	63

Abbreviations

AIT	advanced imaging technology
APR	annual proficiency review
ASAP	aviation screening assessment program
ATSA	Aviation and Transportation Security Act
BDA	behavior detection and analysis
BDO	behavior detection officer
CPER	Chief Performance and Enterprise Risk Office
CREATE	National Center for Risk and Economic Analysis of Terrorism Events
DARMS	dynamic aviation risk management solution

DHS	Department of Homeland Security
EDC	explosives detection canine
EDS	explosives detection system
ETD	explosives trace detection
FAMS	U.S. Federal Air Marshal Service
FTE	full-time equivalent
GPRA	Government Performance and Results Act of 1993
LEO	law enforcement officer
OIG	DHS's Office of Inspector General
OOI	Office of Inspections
ORCA	Office of Requirements and Capabilities Analysis
OSC	Office of Security Capabilities
PSC	passenger screening canine
RTSPA	risk and trade space portfolio analysis tool
SNA	short notice assessment
SOP	standard operating procedure
SPP	Screening Partnership Program
TIP	threat image projection
TSA	Transportation Security Administration
TSIF	Transportation Security Administration Systems Integration Facility
TSO	transportation security officer

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



September 11, 2017

Congressional Requesters:

It has been 16 years since the attacks of September 11, 2001, exposed vulnerabilities in the U.S. aviation system. Since then, the Department of Homeland Security's (DHS) Transportation Security Administration (TSA)—the primary federal agency with responsibility for securing the nation's civil aviation system—has spent billions of dollars on a wide range of programs designed to enhance aviation security. However, achieving TSA's stated mission to protect the nation's transportation systems remains a daunting task. Senior DHS officials have stated that terrorist organizations continue to regard civil aviation as an attractive target for attacks. Further, recent attacks involving aircraft and airports in Egypt, Somalia, Belgium, and Turkey have underscored the continued threat to aviation and the need for an effective aviation security program.

Over the past 5 fiscal years, funding made available to TSA for aviation security has remained relatively steady—ranging from a high of nearly \$7.7 billion in fiscal year 2012 to a low of nearly \$7.0 billion in fiscal year 2013—but fiscal pressures facing the government continue.¹ In this environment of high threat and limited resources, it is essential that TSA identify how to allocate its resources to obtain the greatest risk mitigation value for each dollar spent.

You requested that we review what TSA knows about the costs and effectiveness of its passenger aviation security countermeasures. In this report, we examine

1. the extent that TSA has information on the effectiveness of selected passenger aviation security countermeasures, and what these data indicate, and
2. the extent that TSA has systematically analyzed the cost and effectiveness tradeoffs of alternate combinations of countermeasures within its aviation security system.

¹Estimated funding made available to TSA for aviation security totaled approximately \$7.7 billion in fiscal year 2012, \$7.0 billion in fiscal year 2013, \$7.2 billion in fiscal year 2014, \$7.1 billion in fiscal year 2015, and 7.2 billion in fiscal year 2016.

This report also presents fiscal year 2015 cost and effectiveness information for selected aviation security countermeasures in appendixes I and II, respectively.

This report is a public version of a classified report that we issued in August 2017. TSA deemed some of the information in our August report to be classified or sensitive security information, which must be protected from loss, compromise, or inadvertent disclosure. Therefore, this report omits classified and sensitive security information about the effectiveness of certain aviation security countermeasures and some specifics about TSA's screening procedures. Although the information provided in this report is more limited, the report addresses the same objectives as the classified report and uses the same methodology.

To determine the extent of TSA's information on the effectiveness of its passenger aviation security countermeasures in fiscal year 2015, we reviewed past reports and findings from GAO, TSA, and DHS's Office of Inspector General (OIG) related to the effectiveness of TSA aviation security programs and evidence of steps TSA has taken to address the issues identified. We also asked TSA to provide us with their evidence of the security effectiveness of six selected aviation security countermeasures—passenger prescreening (Secure Flight), checkpoint screening, checked baggage screening, explosives detection canines, the Behavior Detection and Analysis (BDA) program, and the U.S. Federal Air Marshal Service (FAMS)—in detecting, disrupting, and deterring threats to the nation's aviation system. We selected these six passenger aviation security countermeasures because they involve direct interaction with passengers, their belongings, or their personal information and are largely operated and funded by TSA.² We analyzed TSA's performance and testing data to determine the extent of TSA's effectiveness information for these six selected countermeasures and what these data indicate about their security effectiveness during fiscal year 2015—the most recent full year for which data were available. We also reviewed TSA documents related to countermeasure effectiveness such as the results of routine TSA tests of screening technologies deployed at airports.

To obtain TSA perspectives on the extent and reliability of TSA's effectiveness information as well as the effect of any data limitations, we

²Other aviation security countermeasures not included in our review include crew vetting, federal flight deck officers, hardened cockpit doors, cargo screening, and law enforcement officers, among others.

also interviewed senior TSA officials in (1) the Office of Requirements and Capabilities Analysis (ORCA), which is responsible for assessing TSA's operational capability gaps and developing future requirements; (2) the Chief Performance and Enterprise Risk Office (CPER), which is responsible for the overall leadership, vision, and direction for risk management across TSA; (3) the Office of Inspections (OOI), which conducts covert testing of several aviation security countermeasures; and (4) individual program offices associated with each of the six countermeasures.³ We also interviewed officials with the National Center for Risk and Economic Analysis of Terrorism Events (CREATE)—a DHS-funded research center—to obtain their perspective on the challenges TSA faces in measuring the effectiveness of some countermeasures.⁴ We compared TSA's efforts to measure effectiveness to requirements in the Government Performance and Results Act of 1993 (GPRA), as updated by the GPRA Modernization Act of 2010, and leading practices established in GAO's prior work on using performance information to inform management decision making.⁵ We assessed the reliability of TSA's effectiveness data by (1) reviewing TSA documentation of procedures for recording effectiveness data, (2) manually testing for obvious errors and discrepancies in select results, and (3) interviewing knowledgeable TSA officials about procedures for collecting and recording these data. We discuss our findings about the reliability of these data later in this report.

³In November 2016, TSA reorganized and renamed various offices. The Office of the Chief Risk Officer became the Chief Performance and Enterprise Risk Office, and the Office of Security Capabilities was divided into ORCA and the Office of Acquisition Program Management, which is responsible for delivering security capabilities and technologies and for managing the acquisition, testing, deployment and sustainment of TSA's security technology and other acquisition programs.

⁴The National Center for Risk and Economic Analysis of Terrorism Events is a university-based center of excellence funded by the Office of University Programs of the DHS Science and Technology Directorate. The Center's mission is to improve U.S. security through research and development of models and tools to evaluate risks, costs, and consequences of terrorism and natural and manmade hazards, and to guide economically viable investments in homeland security.

⁵See generally Pub. L. No. 103-62, 107 Stat. 285 (1993) (GPRA) and Pub. L. No. 111-352, 124 Stat. 3866 (2011) (updating GPRA); 31 U.S.C. § 1115. The GPRA Modernization Act of 2010 provides an overall framework for assessing agency performance and tools to enhance performance planning and management to inform agency decision making. See also GAO, *Executive Guide: Effectively Implementing the Government Performance and Results Act*, [GAO/GGD-96-118](#) (Washington, D.C.: June 1996). GAO's *Executive Guide* identifies key steps for federal agencies working to successfully implement GPRA.

To determine the extent that TSA officials have systematically analyzed the cost and effectiveness tradeoffs of alternate combinations of countermeasures, we reviewed TSA documentation of their efforts to do so. Specifically, we reviewed technical papers on TSA's Risk and Trade Space Portfolio Analysis tool (RTSPA)—a tool the agency developed to analyze security effectiveness tradeoffs among checkpoint screening and checked baggage screening countermeasures. To learn more about TSA's efforts to analyze cost and effectiveness tradeoffs, we interviewed senior ORCA officials about RTSPA, and observed a demonstration of RTSPA's analytical capabilities. We also met with senior TSA officials including the prior Chief of Staff, and officials in CPER and the Office of Finance and Administration to discuss the agency's efforts to analyze the cost and effectiveness tradeoffs of alternate combinations of countermeasures. We then compared the extent of this analysis to DHS's Policy for Integrated Risk Management memorandum, which describes how DHS components, including TSA, should use risk management to inform strategies, processes and decisions to enhance security.⁶ We also compared the extent of this analysis to TSA's strategic plan.⁷

The performance audit upon which this report is based was conducted from February 2016 to August 2017 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. We worked with DHS from July 2017 to September 2017 to prepare this unclassified version of the original classified report for public release. This public version was also prepared in accordance with these standards.

Background

Enacted in November 2001, the Aviation and Transportation Security Act (ATSA) established TSA as the primary federal agency responsible for

⁶Department of Homeland Security, Secretary of Homeland Security, *DHS Policy for Integrated Risk Management*, Memorandum for all DHS Components (May 27, 2010).

⁷Department of Homeland Security, Transportation Security Administration, *TSA Strategic Plan FY15-FY18* (Washington, D.C.: 2014).

implementing and overseeing the security of the nation's civil aviation system.⁸ In accordance with ATSA, TSA is to ensure that all passengers and property transported by commercial passenger aircraft to, from, or within the United States are adequately screened.⁹ Among other things, TSA is responsible for ensuring that for all flights and flight segments originating in the United States, such screening takes place before boarding and is carried out by a federal government employee except as otherwise permitted in statute.¹⁰ Pursuant to TSA-established policies and procedures in effect at about 440 airports at which TSA performs, or oversees the performance of screening operations (i.e., TSA-regulated airports), all passengers, their accessible property, and their checked baggage are to be screened prior to entering the sterile area of the airport or boarding the aircraft.¹¹ Among other things, these procedures generally provide that passengers pass through security checkpoints where their person, identification documents, and accessible property are screened by Transportation Security Officers (TSO).

Overview of Selected Aviation Security Countermeasures

In this report, we examine six countermeasures specific to aviation security—passenger prescreening (Secure Flight), checkpoint screening, checked baggage screening, explosives detection canines, BDA, and

⁸See Pub. L. No. 107-71, 115 Stat. 597 (2001); 49 U.S.C. § 114(a), (d).

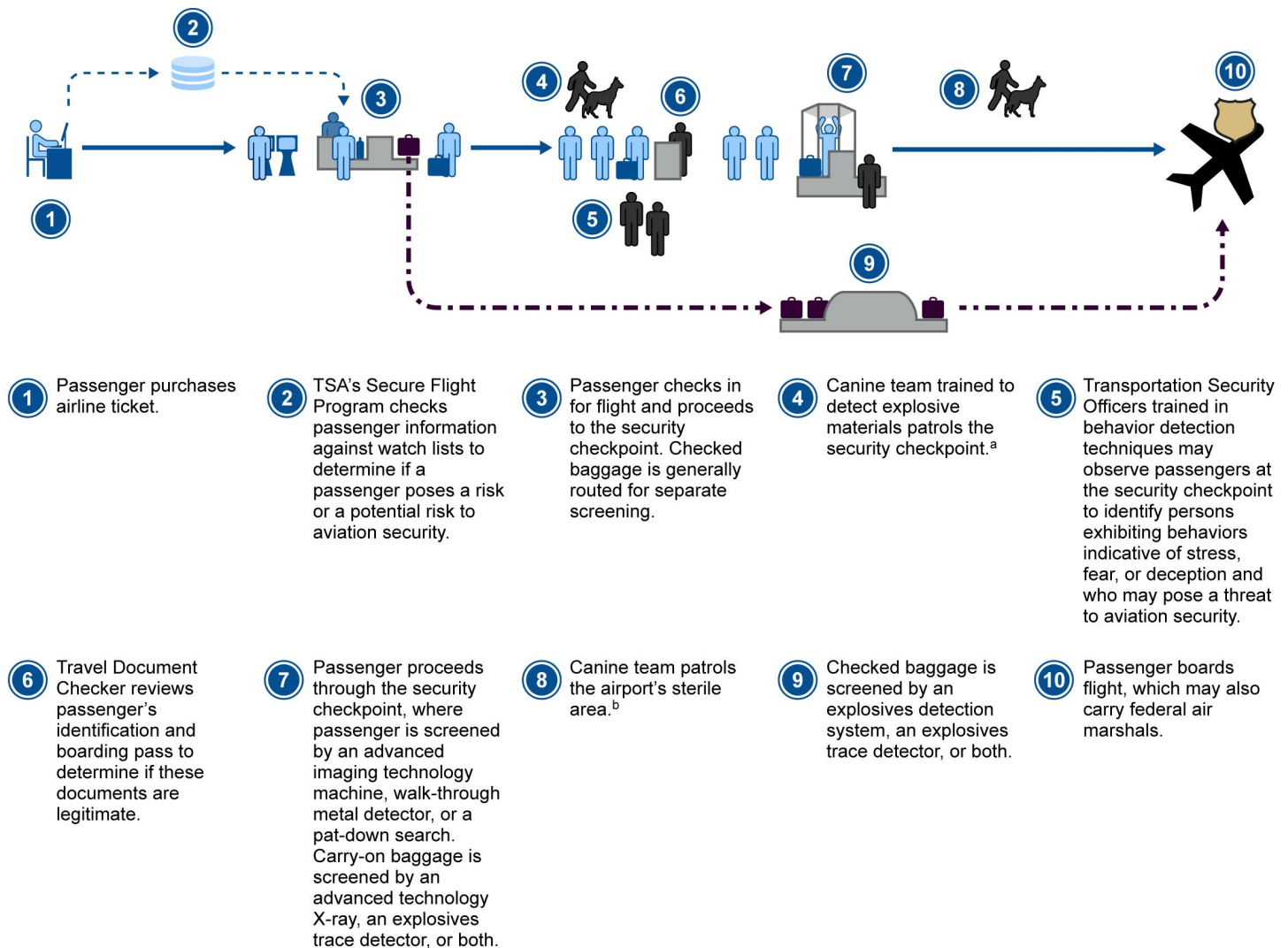
⁹49 U.S.C. § 114(e); 49 C.F.R. pt. 1540. For purposes of this report, “commercial passenger aircraft” generally encompasses the scheduled passenger operations of U.S.-flagged air carriers operating in accordance with their TSA-approved security programs and foreign-flagged air carriers operating in accordance with security programs deemed acceptable by TSA. See 49 C.F.R. pts. 1544 (governing U.S.-flagged air carriers) and 1546 (governing foreign-flagged air carriers).

¹⁰See 49 U.S.C. § 44901. At the 21 airports participating in TSA's Screening Partnership Program (SPP) as of August 2017, TSA has contracted with qualified private-sector entities (SPP contractors) that employ screeners to carry out passenger and baggage screening functions, subject to TSA oversight and in accordance with TSA security standards, procedures and requirements. See 49 U.S.C. § 44920 (authorizing TSA to enter into contracts with private companies to conduct screening activities at TSA-regulated airports). At all other TSA-regulated airports, screening is carried out by a TSA-employed screening workforce—i.e., Transportation Security Officers (TSO). Throughout this report, any reference to TSOs is meant to include screeners employed by SPP contractors unless otherwise noted.

¹¹See 49 C.F.R. § 1540.5 (defining the sterile area of the airport as, in general, an area of an airport that provides passengers access to boarding aircraft and to which access is controlled through the screening of persons and property).

FAMS. An overview of these countermeasures is provided below and figure 1 depicts an illustrative example of the process by which an aviation passenger may encounter these selected countermeasures.

Figure 1: Illustrative Example of a Passenger Experience with Selected Transportation Security Administration (TSA) Countermeasures



Source: GAO analysis of TSA information. | GAO-17-794

Note: This graphic depicts an illustrative example of a passenger experience with selected countermeasures. Not all countermeasures shown are present at all times or at every airport or checkpoint. At airports participating in TSA's Screening Partnership Program, some of these countermeasures may be carried out by employees of private-sector companies under contract with TSA. See 49 U.S.C. § 44920.

^aTSA may also use canine teams to screen passenger property, checked baggage, cargo, and the public areas of the airport.

^bIn general, sterile area refers to an area of an airport that provides passengers access to boarding aircraft and to which access is controlled through the screening of persons and property.

Passenger Prescreening (Secure Flight): TSA uses its Secure Flight prescreening program to match passenger information against federal government watch lists and other information to assign each passenger to one of three risk categories—high risk, low risk, or unknown risk—that either corresponds to the level of screening they will experience at the checkpoint or may deny them an opportunity to board the aircraft. The program requires U.S.- and foreign-flagged commercial aircraft operators traveling to, from, within, or overflying the United States, as well as U.S. commercial aircraft operators with international point-to-point flights, to collect certain information from passengers—such as full name, gender, and date of birth—and transmit that information electronically to TSA.¹²

The Secure Flight program then identifies passengers' risk levels by matching them against federal government watch lists—for example, the No Fly List, comprised of individuals who should be precluded from boarding an aircraft, and the Selectee List, comprised of individuals who should receive enhanced screening at the passenger security checkpoint.¹³ Passengers identified as matching the No Fly List, for example, are precluded from obtaining a boarding pass and proceeding through the screening checkpoint. For passengers matching the Selectee List, air carriers must mark their boarding passes accordingly so TSA can identify them for enhanced screening.

In 2010, TSA began using risk-based criteria to create additional lists for Secure Flight screening, which are composed of high-risk passengers who may not be in the Terrorist Screening Database but whom TSA has determined should be subject to enhanced screening procedures. TSA also began conducting watch list matching against an Expanded Selectee List in order to designate more passengers who are known or suspected

¹²See 49 C.F.R. pt. 1560; see also 73 Fed. Reg. 64,018 (Oct. 28, 2008) (Secure Flight Program Final Rule).

¹³The No Fly and Selectee Lists are subsets of the Terrorist Screening Database—the U.S. government's consolidated watch list of known or suspected terrorists maintained by the Federal Bureau of Investigation's Terrorist Screening Center. Enhanced screening generally includes, in addition to the procedures applied during a typical standard screening experience, a pat-down and an explosives trace detection or physical search of the interior of the passenger's accessible property, electronics, and footwear.

terrorists as selectees for enhanced screening.¹⁴ In addition, as part of TSA Pre✓™—a 2011 initiative to preapprove passengers for expedited screening—TSA uses Secure Flight to screen passengers against several lists of preapproved low-risk travelers. Passengers determined to be eligible for TSA Pre✓™ are identified as such on their boarding passes.¹⁵

Checkpoint Screening: TSA screens individuals and property at airport screening checkpoints to deter and prevent the carriage of any unauthorized or prohibited items on board an aircraft or into the airport sterile area.¹⁶ In general, passengers undergo one of three types of checkpoint screening, based on the Secure Flight determinations shown on boarding passes—standard screening, enhanced screening for selectees, and expedited screening for low-risk passengers. Standard screening typically includes passing through a walk-through metal detector or advanced imaging technology (AIT) machine, which identifies objects or anomalies on the outside of the body.¹⁷ Passengers may also be subject to a pat down if they are screened by the AIT or walk-through metal detector and the equipment alarms.¹⁸ Standard screening also typically includes X-ray screening for the passenger’s accessible property. During X-ray examination of the property, TSOs review the X-ray images, and if potential prohibited items are detected, the property will be manually inspected and screened with an explosives trace detection

¹⁴The Expanded Selectee List includes all records in the Terrorist Screening Database with a full name (first name and surname) and full date of birth that meet the Terrorist Screening Center’s standard to be considered a known or suspected terrorist, but that are not included on the No Fly or Selectee Lists.

¹⁵TSA also uses Secure Flight to conduct TSA Pre✓™ risk assessments—an activity distinct from matching against watch lists—to assign passengers scores based upon their travel-related data, for the purpose of identifying them as low risk for a specific flight.

¹⁶TSOs must deny passage beyond the screening checkpoint to any individual or property that has not been screened or inspected in accordance with passenger screening standard operating procedures. See 49 U.S.C. § 44901(a); 49 C.F.R. §§ 1540.107(a), 1540.111(a)-(b). See also 49 U.S.C. § 44902 and 49 C.F.R. §§ 1544.201(c) and 1546.201(c) (requiring, in general, that air carriers refuse to transport any individual who does not consent to a search or inspection of his or her person and property).

¹⁷TSA standard operating procedures generally afford passengers the option to request screening by a pat down if they so choose in lieu of passing through a walk-through metal detector or AIT machine.

¹⁸Passengers and their accessible property may also be randomly selected for additional screening, which would include a pat down for the passenger and a manual inspection or explosives trace detection (ETD) screening of their accessible property.

(ETD) machine to identify any traces of explosives material.¹⁹ Enhanced screening generally includes, in addition to the procedures applied during a typical standard screening experience, a pat-down and an explosives trace detection or physical search of the interior of the passenger's accessible property, electronics, and footwear. Expedited screening typically includes walk-through metal detector screening and X-ray screening of the passenger's accessible property, but unlike in standard screening, travelers do not have to, among other things, remove their belts, shoes, or light outerwear.

Checked Baggage Screening: TSA inspects passengers' checked baggage to deter, detect, and prevent the transport of any unauthorized explosive, incendiary, or weapon onboard an aircraft.²⁰ Checked baggage screening is accomplished through the use of explosives detection systems (EDS)—which use X-rays with computed tomography technology to automatically measure the physical characteristics of objects in baggage and trigger an alarm when objects that exhibit the physical characteristics of explosives are detected—and ETD machines, which use chemical analysis to manually detect traces of explosive materials' vapors and residue. At airports with EDS, EDS machines are generally employed for primary screening of checked baggage while ETD machines are used for secondary screening to help resolve questions raised by EDS screening. At airports without EDS machines, ETDs are used as the primary method for screening checked baggage.

Explosives Detection Canines: TSA's National Explosives Detection Canine Team Program trains, deploys, and certifies explosives detection canine teams in order to deter and detect the introduction of explosive devices into U.S. transportation systems. Each canine team consists of a handler paired with a canine trained in explosives detection. The canine handlers are generally either a state or local law enforcement officer

¹⁹To provide passengers with guidance on the types of items TSA policy prohibits from being carried onto an aircraft, TSA maintains a Prohibited Items List that lists items passengers may not carry into the sterile area or onboard an aircraft, which is available through TSA's website at <https://www.tsa.gov/travel/security-screening/prohibited-items>. The list is not exhaustive, but rather includes examples and categories of items that are prohibited, and TSOs may use their discretion to prohibit items they deem could pose a threat to transportation security.

²⁰See 49 U.S.C. § 44901(a), (d); 49 C.F.R. § 1540.111(c). See also 49 U.S.C. § 44902 and 49 C.F.R. § 1544.203(e) and 1546.203(b) (requiring, in general, that air carriers refuse to transport any individual's checked baggage or property if the individual does not consent to a search or inspection of that checked baggage or property).

(LEO) or a TSA employee. Two types of LEO teams and two types of TSA-based teams were trained to operate in the aviation environment during fiscal year 2015. First, TSA explosives detection canine teams patrol terminals, curbside areas, and other airport environments while TSA passenger screening canine teams primarily search for explosives odor on passengers in airport terminals. Second, LEO aviation teams patrol airport terminals, curbside areas, and sterile areas while LEO multimodal teams operate in the airport environment and screen air cargo but also operate in mass transit and maritime environments.

Behavior Detection and Analysis: TSA's BDA program employs behavior detection officers (BDO) at passenger screening checkpoints to identify potential threats by observing individuals for certain behavioral indicators—behaviors indicative of stress, fear, or deception. These behavioral indicators include, for example, assessing the way an individual swallows or the degree to which an individual's eyes are open. According to TSA, these verbal and nonverbal cues and behaviors may indicate mal-intent, such as the intent to carry out a terrorist attack, and provide a means for TSA to identify passengers who may pose a risk to aviation security and refer them for additional screening. During this referral screening, if passengers exhibit additional such behaviors, or if other events occur, such as the discovery of a suspected fraudulent document, BDOs are to refer these passengers to a LEO for further investigation. In fiscal year 2015, the program deployed BDOs primarily in teams of two at passenger screening checkpoints. However, TSA officials reported that in the summer of 2016, the agency began taking steps to integrate BDOs into the TSO workforce by assigning BDOs to the travel document checker position and other positions at passenger screening checkpoints where they are able to observe and interact with passengers in the performance of their screening duties.²¹

U.S. Federal Air Marshal Service: FAMS deploys federal air marshals on passenger flights to detect, deter, and defeat hostile acts targeting U.S. air carriers, airports, passengers, and crews. In accordance with

²¹TSA officials reported that they made this change partially in response to a requirement in the Aviation Security Act of 2016, which was enacted on July 15, 2016, as title III of the Federal Aviation Administration's Extension, Safety, and Security Act of 2016. See Pub. L. No. 114-190, § 3304(a)(1), 130 Stat. 615, 655 (2016). Specifically, the Act required that TSA, not later than 30 days after enactment, utilize BDOs for passenger and baggage security screening, including the verification of traveler documents, particularly at designated TSA Pre✓™ lanes to ensure that such lanes are operational for use and maximum efficiency. Id.

ATSA, as amended, TSA is authorized to deploy federal air marshals on every passenger flight of a U.S. air carrier and is required to deploy federal air marshals on every such flight determined by the Secretary of Homeland Security to present high security risks, with nonstop, long-distance flights, such as those targeted on September 11, 2001, considered a priority.²² One of FAMS's top priorities is to deploy air marshals on flights that have a known or suspected terrorist on board. When FAMS assigns air marshals to cover such flights, it refers to these flights as special mission coverage assignments.

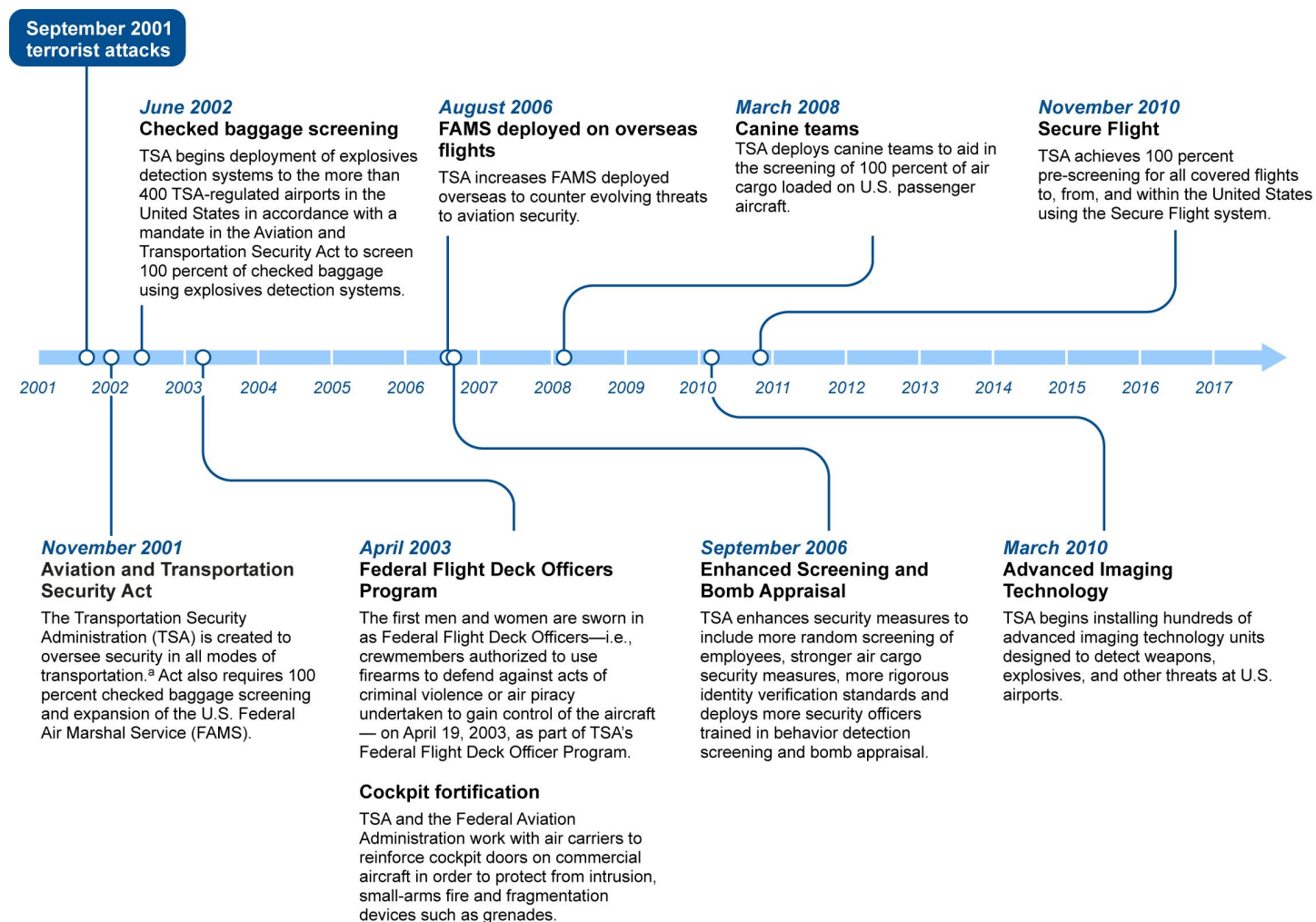
TSA's System of Aviation Security Countermeasures

TSA uses a risk management strategy—referred to as “layers of security”—whereby TSA simultaneously deploys a mix of screening and other security countermeasures to deter and detect threats. TSA deploys countermeasures in varying combinations at each airport based on available resources, specific security concerns, and the airport's risk category, among other things. Since the terrorist attacks of September 11, 2001, TSA has implemented and added countermeasures, and refined security procedures in response to specific attacks or threats—such as the liquid explosives plot in 2006.²³ Figure 2 depicts examples of this progression, illustrating the addition or enhancement of certain TSA countermeasures over the years.

²²See 49 U.S.C. § 44917(a)(1)-(2),(b).

²³In 2006, terrorist cells in Great Britain planned to carry bomb materials—including liquid explosives—on flights from London to cities in the United States and Canada. These materials were to be assembled and detonated while in flight. Police were able to learn of the plot and arrest the plotters before any attacks were carried out.

Figure 2: Examples of Aviation Security Countermeasures Deployed or Expanded, 2001-2017



Source: GAO analysis of TSA information. | GAO-17-794

Note: Since 2010, TSA has taken additional steps to enhance and expand the deployment of some countermeasures.

^aSee Pub. L. No. 107-71, 115 Stat. 597 (2001).

TSA Has Effectiveness Data on Some Countermeasures That Show Mixed Results, But Does Not Measure Deterrence

Data on the Effectiveness of Selected Countermeasures in Detecting and Disrupting Threats to Aviation Security Vary in Extent and Reliability

TSA collected fiscal year 2015 data on the effectiveness of four of the six countermeasures we selected—passenger prescreening, checkpoint screening, checked baggage screening, and explosives detection canines—in detecting or disrupting threats to passenger aviation security.²⁴ TSA assesses this effectiveness differently for each of these four countermeasures. For example, TSA assessed the effectiveness of its passenger prescreening countermeasure in detecting passengers that may pose a threat to aviation security by measuring the percentage of airline passenger records vetted through its Secure Flight system and the number of high-risk passengers identified. In contrast, TSA assessed the effectiveness of its canine program in detecting and disrupting potential security threats by measuring canine-handler team performance during their annual certification tests as well as covert scenario-based tests called short notice assessments (SNA).

Some of the effectiveness data TSA has for fiscal year 2015 are of limited reliability and TSA is taking steps to improve this information. For instance, we reported in September 2016 that checkpoint and checked baggage screening effectiveness data from TSA’s Aviation Screening Assessment Program (ASAP) Advantage covert tests conducted in fiscal year 2015 were not reliable.²⁵ Specifically, TSA found that TSOs

²⁴It is TSA’s goal to detect, disrupt, and deter threats to the nation’s civil aviation system. When we discuss effectiveness throughout this report, we mean effectiveness in detecting, disrupting, and deterring threats, unless otherwise noted.

²⁵GAO, *Aviation Security: TSA Should Ensure Testing Data Are Complete and Fully Used to Improve Screener Training and Operations*, [GAO-16-704](#) (Washington, D.C.: Sept. 7, 2016). ASAP tests are covert tests conducted by TSA at both screening checkpoints and checked baggage screening areas. ASAP tests are to be implemented locally by unrecognizable role players who attempt to pass threat objects, such as knives, guns, or simulated improvised explosive devices, through the screening checkpoints or onto the plane in their checked baggage. The tests are designed to assess the operational effectiveness of TSOs.

performed more poorly in ASAP tests conducted by an independent contractor than in the same tests conducted by local TSA personnel at the same airports.²⁶ This raised questions about the validity of ASAP tests conducted by local TSA personnel and indicated that TSA's fiscal year 2015 ASAP pass rates likely showed a higher level of TSO performance in screening for prohibited items than was actually the case. In response to this issue, and to provide ongoing quality assurance for field-based covert testing results, in April 2016, TSA began deploying headquarters-based covert testing teams in both the checkpoint and checked baggage screening environments.²⁷ TSA officials stated that comparing the results of field- and headquarters-based tests provides TSA with a useful indication of whether or not the field-based covert testing results are valid.²⁸

In another example, we determined that fiscal year 2015 SNA data were not reliable for the purpose of reporting explosives detection canine teams' covert testing pass rates. Specifically, in the course of our review we found that these data included duplicate entries and errors, and TSA officials stated that the results of an unknown number of SNAs may not have been recorded. Further, we found that TSA's data collection process for SNA results that were recorded lacked procedures to ensure that manually entered data were accurate and complete. To address these data limitations, canine program officials stated that a new process was implemented in October 2016 to incorporate SNA results directly into the Canine Website System—a central electronic management database for various canine program data. According to these officials, this new

²⁶According to TSA, the goals of the independent covert testing done by the contractor were to (1) establish a baseline of expected TSO performance, (2) assess the ASAP program, (3) validate the accuracy of historical ASAP data, and (4) capture and record sources of officer failure to follow procedures and detect threats and identify the root causes of the failures to follow procedure.

²⁷According to TSA officials, TSA conducts roughly 8,000 field-based and 4,000 headquarters-based covert tests each year and plans to continue conducting these test in future years. These tests have replaced the ASAP Advantage program.

²⁸TSA also has begun using a new Task Process Factors tool, which collects additional data on the type of threat being tested during headquarters-based and field-based testing, the environmental factors present during the time of the test, and the root causes of any failures, among other things. According to TSA officials, the Task Process Factors tool allows TSA to quickly and easily disseminate standardized covert testing data that are essential for understanding weaknesses and vulnerabilities in TSA's screening system to TSA leadership as well as airports across the country. TSA officials report that, among other uses, these data can be used to better inform TSA's corrective actions and training priorities.

process will better ensure that SNA data are complete, accurate, and reliable for use by program officials and TSA leadership in evaluating the effectiveness of the program. Appendix II presents specific fiscal year 2015 effectiveness data for the four selected countermeasures for which TSA had effectiveness information.

During fiscal year 2015, TSA did not collect data on the effectiveness of two of the six countermeasures we selected—FAMS and the BDA program—in detecting and disrupting threats to aviation security. For FAMS, TSA officials explained that it is very difficult to empirically measure the effectiveness of federal air marshals and the program has no efforts underway to collect such data.²⁹ We discuss this issue later in this report.

For the BDA Program, we reported in November 2013 that TSA had not demonstrated that BDOs could consistently identify the behavioral indicators and, further, that decades of peer-reviewed, published research on the complexities associated with detecting deception through human observation also called into question the scientific basis for TSA's behavior detection activities.³⁰ As a result, we recommended that TSA limit future funding for the agency's behavior detection activities until TSA can provide scientifically validated evidence that demonstrates that behavioral indicators can be used to identify passengers who may pose a threat to aviation security. DHS did not concur with the recommendation but has since reduced funding for the BDA Program and taken steps to begin to assess program effectiveness.³¹ For example, in 2014 TSA revised its list of behavioral indicators and contracted for a literature review to identify additional sources of evidence supporting these

²⁹FAMS uses a single performance measure called the "composite index of FAMS risk-based flight coverage goals" to assess the extent to which it has met its flight coverage and resource use targets. The index, while not a measure of effectiveness, is a composite score reflecting FAMS's performance in meeting its flight coverage and resource allocation targets across multiple categories of flights, including air marshal coverage of certain domestic and international flights.

³⁰GAO, *Aviation Security: TSA Should Limit Future Funding for Behavior Detection Activities*, [GAO-14-159](#) (Washington, D.C.: Nov. 8, 2013).

³¹TSA officials have stated that our recommendation was one of several factors in DHS's decision to support a reduction in the number of full-time equivalent (FTE) BDOs by 471—from the 3,131 BDO FTEs that DHS requested and funded in fiscal years 2013 through 2015 to 2,660 BDO FTEs requested in fiscal year 2016. In fiscal year 2016, this reduced number of BDO FTEs represented a reduction in annual operating costs of about \$35.4 million.

indicators.³² However, in July 2017, we reported that in our review of all 178 sources TSA cited in support of its revised list, we found that 98 percent (175 of 178) did not provide valid evidence applicable to the specific indicators TSA identified them as supporting.³³ Based on our findings, we continue to believe that TSA should limit future funding for the agency's behavior detection activities until TSA can provide valid evidence that demonstrates that behavioral indicators can be used to identify passengers who may pose a threat to aviation security, as we recommended in our November 2013 report.

Table 1 identifies whether TSA has information on the effectiveness of the six selected countermeasures in detecting and disrupting threats to aviation security during fiscal year 2015, the data limitations we identified, and steps TSA officials have taken to improve this effectiveness information.

³²In October 2016, TSA also began conducting a covert assessment to collect data on the effectiveness of BDOs in identifying certain behavioral indicators that may be indicative of stress, fear, or deception. As of August 2017, TSA had conducted a first phase of the covert testing at four airports but had no plans for additional testing at that time.

³³GAO, *Aviation Security: TSA Does Not Have Valid Evidence Supporting Most of the Revised Behavioral Indicators Used in Its Behavior Detection Activities*, [GAO-17-608R](#) (Washington, D.C.: July 20, 2017).

Table 1: Transportation Security Administration (TSA) Information about Selected Countermeasure Effectiveness in Detecting and Disrupting Threats to Aviation Security in Fiscal Year 2015

Aviation Security Countermeasure	Does TSA Have Effectiveness Information?	Limitations Identified by GAO	Steps TSA has taken to Improve Effectiveness Data
Passenger Prescreening (Secure Flight)	Yes	TSA does not have a means to measure false negatives, instances where individuals on a watch list used by TSA were not identified during prescreening	TSA has hired a contractor to assess the effectiveness of the Secure Flight system, which should provide a better understanding of the system's capability to minimize the occurrence of false negatives. ^a
Checkpoint Screening	Yes	Aviation Screening Assessment Program (ASAP) covert testing results on checkpoint screening are not reliable due to discrepancies in test results, and Threat Image Projection (TIP) data are incomplete because not all airports submitted TIP scores ^b	TSA has implemented both headquarters- and field-based covert tests for checkpoint screening to better ensure reliable results. TSA is also tracking airports for which monthly TIP data has not been submitted and has begun implementing a revised directive to help airports meet their TIP requirements.
Checked Baggage Screening	Yes	Discrepancies in fiscal year 2016 ASAP covert testing results for checked baggage indicate that fiscal year 2015 results for these same tests may also be unreliable ^c	As with checkpoint screening, TSA has also implemented headquarters- and field-based covert tests to better ensure reliable results.
Explosives Detection Canines	Yes	Covert testing results from Short Notice Assessments (SNA) may not be complete or accurate ^d	To better ensure that data are complete, accurate, and reliable, TSA has implemented a new process to improve how it collects, records, and maintains SNA results.
Behavior Detection & Analysis (BDA)	No	TSA does not have information on the effectiveness of its BDA program	TSA has conducted a literature review but has not yet identified valid evidence that demonstrates that behavioral indicators can be used to identify passengers who may pose a threat to aviation security.
U.S. Federal Air Marshal Service (FAMS)	No	TSA does not have information on the effectiveness of FAMS	FAMS officials stated that one of the program's primary security contributions is to deter threats to aviation security, but measuring this deterrent effect is challenging. TSA does not have an effort underway to do so.

Source: GAO analysis of TSA data. | GAO-17-794

Note: This table presents the extent of TSA's information on the fiscal year 2015 effectiveness of the six selected countermeasures in detecting and disrupting threats to passenger aviation security. TSA does not have information on the deterrent effect of any of its aviation security countermeasures.

^aTSA's Secure Flight system screens passengers against the No Fly, Selectee, and other lists of high-risk individuals to identify travelers who should receive enhanced screening at airport checkpoints or be denied boarding.

^bThe TIP system is designed to test TSOs' detection capabilities by projecting threat images, including images of guns and explosives, into passengers' carry-on bags as they are screened at the checkpoint. TSOs are responsible for positively identifying the threat image and calling for the bag to be searched. In September 2016, we found that TSA's TIP data from fiscal year 2009 to 2014 was incomplete as TSA could not provide TIP scores for every airport during this period. We recommended that TSA officials at individual airports submit complete TIP results to the TSA national database as required and that TSA conduct analysis of national TIP data for trends that could inform training needs and improve future training and TSO performance assessments. TSA concurred with our recommendations and is taking steps to address them. Specifically, a new TIP Operations Directive was implemented in October 2016 to disseminate procedures for performance data collection and submission to improve TIP data. According to agency officials, the number of non-compliant airports decreased during fiscal year 2016. However, since these improvements occurred during fiscal years 2016 and 2017, fiscal year 2015 TIP data remained incomplete and unreliable for the purposes of assessing TSOs' effectiveness at identifying TIP images. See GAO, *Aviation Security: TSA Should Ensure Testing Data Are Complete and Fully Used to Improve Screener Training and Operations*, [GAO-16-704](#) (Washington, D.C.: September 2016).

^cIn fiscal year 2015, TSA hired a contractor to independently perform ASAP covert testing on checkpoint screening at 40 airports and found that TSOs performed more poorly in ASAP tests conducted by the contractor personnel as compared to ASAP tests conducted by local TSA personnel. This indicated that TSA's reported fiscal year 2015 ASAP pass rates were likely showing a higher level of performance than was actually the case. However, the contractor did not perform ASAP covert tests on checked baggage screening. Therefore, TSA does not have independent data to validate its covert testing results on checked baggage screening during fiscal year 2015 and TSA officials stated that they cannot be certain these data are reliable.

^dSNAs are covert tests conducted by TSA's canine program to assess canine teams' operational effectiveness in detecting and responding to possible explosives.

TSA Effectiveness Data on Selected Countermeasures Indicate Mixed Results

Some of TSA's fiscal year 2015 data indicate countermeasure effectiveness while other data highlight vulnerabilities in the agency's ability to detect and disrupt threats to aviation security. For example, for the passenger prescreening countermeasure, TSA officials reported that in fiscal year 2015, TSA's Secure Flight program vetted 100 percent of the more than 816 million records of passengers who flew into, out of, over, or within the United States, and on U.S.-flagged aircraft operating internationally point-to-point. In addition, for the checkpoint and checked baggage countermeasures, TSA uses Annual Proficiency Reviews (APR) to evaluate TSOs' skill in performing various checkpoint and checked baggage screening functions, such as pat downs of passengers, bag searches, and use of explosives detection equipment.³⁴ In 2015, the

³⁴In accordance with ATSA, TSA requires that TSOs pass the Annual Proficiency Review to continue to remain employed in that capacity. See 49 U.S.C. § 44935(f)(5). If a TSO does not pass one of the components of the APR after two or, in some cases, three attempts, they are subject to removal from their position. According to TSA, more than 97 percent of the TSO workforce required to take the APR did so in calendar year 2015. The remaining nearly 3 percent did not take the APR due to being out on leave without pay, workers' compensation, or deployed on Military Duty, among other reasons.

average rate at which TSOs passed all APR component tests on the first try was nearly 95 percent.³⁵

On the other hand, some fiscal year 2015 effectiveness data indicate vulnerabilities. For example, results from covert testing conducted by TSA's OOI during fiscal year 2015 indicate vulnerabilities in the checkpoint and checked baggage screening systems. Specific details about OOI's test results are omitted because the information is classified.

TSA Does Not Measure Deterrence for Any of Its Aviation Security Countermeasures

While TSA has methods to measure its effectiveness in detecting and disrupting threats, the agency has no such methods to measure progress toward its goal of deterring attacks on the U.S. aviation system. TSA officials have cited the deterrent effect of various countermeasures—including FAMS, canine teams, BDOs, and AIT machines—but does not have information on the deterrent effect of any of these countermeasures. For example, TSA officials explained that canine teams that patrol airports—searching unattended bags and unattended vehicles, among other activities—provide a deterrent presence at airports, but officials noted that they do not have any data on these canines' deterrent effect. Most notably, with regard to FAMS, TSA officials explained that one of the primary security contributions and a key aspect of the FAMS's mission is to deter attacks. However, FAMS officials explained that they do not have information on FAMS's deterrent effect because it is difficult to model, measure, and quantify. TSA officials in multiple offices explained that this difficulty applies not just to FAMS, but also to other TSA countermeasures with an intended deterrent effect.

OMB and GAO have acknowledged the difficulty in measuring the effect of deterrence programs, but have identified options to overcome these challenges. OMB guidance recognizes that programs with a deterrence or prevention focus can be difficult to measure and suggests that proxy measures that are closely tied to the outcome can be used to determine how well a deterrence process is functioning.³⁶ We have similarly

³⁵Beginning in calendar year 2015, TSA changed its APR testing cycle from fiscal year to calendar year. As a result, we present calendar year 2015 APR data in this report.

³⁶Office of Management and Budget, *Performance Measurement Challenges and Strategies* (Washington, D.C.: June 18, 2003).

acknowledged such methodological challenges and identified alternate evaluation methods that could be helpful to agencies, such as using simulations.³⁷ TSA could, for example, develop theoretical game scenarios and have testers simulate would-be attackers' decisions when attempting to carry out an attack on the aviation system. Officials with CREATE—a DHS-funded research center—told us that they have conducted some conceptual research on the value of deterrence and believe it would be possible to assess TSA's deterrent effect by, for example, allowing covert testers to choose their method of attack. Such an assessment could provide TSA with insights regarding which countermeasures a would-be attacker might choose to avoid in various scenarios.

In a March 2016 report prepared for TSA, CREATE analyzed a prospective risk-based security initiative TSA had begun developing and highlighted the need for further research into deterrence including the need to model the economic value of deterrence.³⁸ CREATE officials explained that they highlighted this issue because in a resource constrained environment, optimizing TSA's deterrent effect may be a more cost effective solution to aviation security threats than focusing solely on detection and interdiction. A senior official with CPER stated that the office believes there is value in pursuing further research regarding deterrence and noted that the office had included a request for funding to study deterrence in its fiscal year 2017 expenditure plan, but the request was on hold due to limited funding.

In accordance with GPRA, as updated by the GPRA Modernization Act, agencies are to establish performance measures to assess progress toward goals.³⁹ Measuring performance allows organizations to track the progress they are making toward their goals and gives managers critical

³⁷GAO, *Designing Evaluations: 2012 Revision*, [GAO-12-208G](#) (Washington, D.C.: January 2012).

³⁸The National Center for Risk and Economic Analysis of Terrorism Events, *Dynamic Aviation Risk Management Solution (DARMS): Research Study to Demonstrate a Proof-of-Concept*, Mar. 14, 2016, a report prepared for TSA. In 2014, TSA began exploring the idea for DARMS—a comprehensive, holistic aviation security system that would assess risk on a per-flight basis and allow TSA to dynamically adjust its countermeasures in response. However, according to CPER officials, TSA elected not to fund the \$1 million cost of developing a DARMS implementation plan in its fiscal year 2018 budget.

³⁹See generally Pub. L. No. 103-62, 107 Stat. 285 (1993) (GPRA) and Pub. L. No. 111-352, 124 Stat. 3866 (2011) (updating GPRA); 31 U.S.C. § 1115.

information on which to base decisions for improving their progress.⁴⁰ For example, they can use performance information when developing strategies, allocating resources, identifying problems, and taking corrective action.⁴¹

TSA officials told us that developing a means to assess TSA's deterrent effect would be difficult and require a multi-year effort but having such a means would be helpful. For example, TSA's prior Chief Risk Officer told us that TSA's countermeasures deter nefarious actors from attempting an attack on an aircraft, but better understanding this concept will be critical to TSA in its transition into a more holistic, system-wide approach to aviation security. Additionally, a senior ORCA official explained that a better understanding of the deterrent effect of TSA countermeasures could help TSA optimize use of its resources. For example, this official noted that there may be a point at which adding additional federal air marshals has diminishing returns in terms of deterrence and better understanding FAMS's deterrent effect could help TSA identify that point. This official further stated that developing a method to assess deterrence for this purpose would be challenging but feasible.

In the absence of any systematic or methodological approach to assessing TSA's deterrent value, TSA officials have relied on theories of causality and limited evidence available from U.S. intelligence sources. For example, FAMS officials cited the fact that there has not been a hijacking on a U.S. carrier since 2002 as evidence of FAMS's deterrent effect, but had no specific evidence to support FAMS's contribution to this outcome. In another example, ORCA officials noted that a 2014 article in an online magazine published by al-Qaeda encouraging would-be-attackers to avoid airports with a certain countermeasure provided evidence of its deterrent value. These observations may provide limited insight into TSA's deterrent effect, but developing a method to systematically assess the deterrent effect of TSA's security efforts would better position TSA to improve progress toward its goal—deterring attacks on the U.S. aviation system.

⁴⁰GAO, *Executive Guide: Effectively Implementing the Government Performance and Results Act*, [GAO/GGD-96-118](#) (Washington, D.C.: June 1996).

⁴¹GAO, *Managing For Results: Enhancing Agency Use of Performance Information for Management Decision Making*, [GAO-05-927](#) (Washington, D.C.: Sept. 9, 2005).

TSA Can Compare the Effectiveness of Certain Combinations of Aviation Security Countermeasures, but Does Not Systematically Analyze Cost and Effectiveness Tradeoffs Across All Countermeasures

TSA Has a Tool to Assess the Security Effectiveness of Alternate Combinations of Some Countermeasures

In 2014, TSA's ORCA began using a Risk and Trade Space Portfolio Analysis Tool (RTSPA) to analyze the security effectiveness of alternate combinations of some aviation security countermeasures for the purpose of informing TSA acquisition and deployment decisions. RTSPA provides a means for TSA to model its security effectiveness in different scenarios. For example, the tool could be used to compare the security effectiveness of a theoretical airport screening checkpoint with canines to that of a checkpoint modeled without canines.⁴²

According to ORCA officials, they developed RTSPA to assess security effectiveness tradeoffs among countermeasures that they believed would most benefit from the detailed quantitative analyses that the tool provides, rather than across TSA's entire system of aviation security countermeasures. Specifically, TSA officials explained that RTSPA is designed to analyze tradeoffs among checkpoint screening countermeasures—including canine teams and BDOs—and checked baggage screening, but was not developed to analyze tradeoffs among other countermeasures TSA deploys. For example, ORCA officials told us that the tool was not developed to analyze crew vetting or FAMS because understanding the security tradeoffs of these countermeasures, while important, does not require the use of such a resource intensive tool like

⁴²In developing this tool, TSA officials reviewed existing countermeasure effectiveness data, including covert test results, laboratory and field testing data, and threat information and converted it into comparable units. To distill a single quantified metric for the effectiveness of a canine at the checkpoint, for example, TSA analyzed effectiveness data from operational tests and evaluations performed by DHS's Science and Technology Directorate. For countermeasures where effectiveness data were not available, such as BDOs, ORCA relied on qualitative subject matter expert assessments to inform RTSPA assumptions about the effectiveness of these countermeasures.

RTSPA.⁴³ In addition, RTSPA does not account for the full system of aviation security countermeasures, including countermeasures such as hardened cockpit doors and Federal Flight Deck Officers—flight crew members authorized and trained to use firearms.⁴⁴ ORCA officials further explained that in 2014, when initially developing the tool, they also developed comparable countermeasure cost data to allow for cost-effectiveness comparisons among countermeasures. However, ORCA officials report that they subsequently stopped analyzing cost tradeoffs because they believed other TSA offices could conduct such analysis.

In the last two years, TSA officials have used the results of RTSPA analyses to inform some resource tradeoff decisions. For example, ORCA officials told us that in 2015, TSA leadership used the results of a RTSPA analysis when considering options for improving overall security effectiveness at airports that did not have AIT machines. Specifically, TSA used RTSPA to consider the level of risk and potential risk mitigation value of alternative security measures at these airports. TSA officials report that this RTSPA analysis contributed to TSA's decision to deploy 146 additional AIT machines to such airports. In another example, ORCA officials noted that in early 2017, they used RTSPA to analyze options for resolving checked baggage alarms, taking into consideration the relative risks of military-grade explosive materials and homemade explosive devices.

TSA officials stated that their use of RTSPA has been limited to date because it is still a relatively new tool. However, ORCA officials told us that they expect use of the tool's analysis to grow as the agency increasingly seeks to use analytic tools to inform acquisition and deployment decisions. As such, ORCA officials plan to update RTSPA and expand its analytical capabilities.⁴⁵

⁴³TSA's crew vetting program matches names of aircraft pilots and flight and cabin crew against terrorist watch lists.

⁴⁴It is also important to note that RTSPA is designed to analyze the effectiveness of select countermeasures in detecting explosives, but not firearms, biohazards, or other weapons.

⁴⁵ORCA officials told us that future iterations of RTSPA may include additional capabilities.

TSA Has Not Systematically Analyzed Potential Cost and Effectiveness Tradeoffs Across the Entire System of Aviation Security Countermeasures

TSA does not have any efforts underway to systematically evaluate the potential cost and effectiveness tradeoffs across the full aviation security system. Although TSA's use of RTSPA to identify effectiveness tradeoffs among selected countermeasures provides some such information, the tool's analyses are limited and the tool is not designed to offer a system-wide view of effectiveness. When we asked TSA's prior Chief of Staff about any such efforts, he stated that TSA had not systematically evaluated cost and effectiveness tradeoffs because TSA's aviation security system is constantly evolving to meet emerging threats, and assessing a system in flux is challenging. However, he told us that such an analysis would be helpful.

DHS policy and TSA's strategic plan call for the systematic evaluation of the costs and effectiveness of TSA's chosen mix of aviation security countermeasures. Specifically, DHS's 2010 Policy for Integrated Risk Management calls on components, including TSA, to evaluate the performance of risk management strategies it decides to implement.⁴⁶ In the case of TSA, TSA's chosen mix of aviation security countermeasures represents TSA's current risk management strategy. The policy further establishes that components should develop and analyze alternative strategies to manage risks by considering the projected costs, benefits, and ramifications of each alternative. In addition, TSA's current Strategic Plan establishes the goal of increasing efficiency and operational effectiveness through disciplined processes and dynamic resource management.⁴⁷ One of the stated outcomes associated with this goal is the ability to effectively optimize resource allocation to strike a balance of costs, benefits, and risk. In addition, it was the stated objective of ORCA's predecessor—the Office of Security Capabilities (OSC)—to develop and implement a comprehensive tradeoff analysis across the security system

⁴⁶Department of Homeland Security, Secretary of Homeland Security, *DHS Policy for Integrated Risk Management*, Memorandum for All DHS Components (May 27, 2010).

⁴⁷Department of Homeland Security, Transportation Security Administration, *TSA Strategic Plan FY15-FY18* (Washington, D.C.: 2014).

to inform investment decisions.⁴⁸ OSC's strategic plan further states that such an analysis would include a full set of strategic choices TSA should consider when determining how to respond to a threat or making an investment decision, helping to determine which alternatives provide the greatest risk mitigation value for each dollar spent.

A senior ORCA official explained that while there is a need for a system-wide tradeoff analyses, RTSPA alone may not be the right tool for this. This official explained that TSA may not require detailed quantitative analyses from a resource-intensive tool such as RTSPA to understand the effectiveness tradeoffs among all aviation security countermeasures, and a portfolio of tools of varying precision and depth could be used to obtain a system-wide view. This official noted that developing TSA's capability for system-wide tradeoff analysis would be challenging and require a multi-year effort. However, RTSPA could serve as a useful starting place for a more comprehensive system-wide analysis. For example, TSA could build upon ORCA's past efforts to analyze the comparative cost effectiveness of countermeasures and its experience isolating the security effectiveness contributions of individual countermeasures.

Without a systematic analysis of the cost and effectiveness tradeoffs across aviation security countermeasures TSA is limited in its ability to achieve its stated goal of optimizing resource allocation and striking a balance of costs, effectiveness, and risk across the system. In an environment of constrained resources and continuing threats to aviation security, producing such analysis could assist TSA leadership in targeting its limited resources to achieve the greatest system-wide risk mitigation value for each dollar spent.

⁴⁸Department of Homeland Security, Transportation Security Administration, Office of Security Capabilities, *Strategic Plan 2013-2016* (Washington, D.C.: 2013). In November 2016, TSA reorganized and renamed various offices. The Office of Security Capabilities was divided into the Office of Requirements and Capabilities Analysis, which is responsible for assessing TSA's operational gaps and developing future requirements and the Office of Acquisition Program Management, which is responsible for managing the acquisition, testing, deployment and sustainment of TSA's security technology and other TSA acquisition programs. TSA officials told us that as of August 2017, ORCA has not yet developed a updated strategic plan identifying new goals and objectives.

Conclusions

Since the terrorist attacks of September 11, 2001, TSA has spent billions of dollars on a range of aviation security programs with the goal of detecting, disrupting, and deterring threats. However, TSA does not have a complete understanding of the contributions these programs are making to this goal. Specifically, TSA has some information on how well it can detect and disrupt threats and is taking steps to improve this information, but does not have information on its ability to deter attacks—a key component of TSA’s goal. For example, in fiscal year 2015, TSA spent approximately \$800 million on FAMS—a program with a focus on deterring attacks on aircraft—yet the agency has no information on its effectiveness in doing so. While we and OMB have acknowledged the difficulty in measuring deterrence, we have also suggested options to overcome these challenges. Further, in accordance with GPRA, as updated by the GPRA Modernization Act, agencies are to assess the effectiveness of their programs and leading practices established in GAO’s prior work stress the importance of agencies tracking progress toward goals. Developing a method to assess the deterrent effect of aviation security countermeasures would better position TSA to improve progress toward a key goal—deterring attacks on the U.S. aviation system.

Since September 11, 2001, TSA has added countermeasures and refined security procedures in response to specific attacks or threats, but has not systematically evaluated its chosen combination of aviation security countermeasures as called for in DHS policy and TSA’s strategic plan. Specifically, TSA does not have any efforts underway to evaluate the potential cost and effectiveness tradeoffs across the full aviation security system because, according to a senior TSA official, the aviation security system is constantly evolving in response to emerging threats, and assessing a system in flux is challenging. However, it is using a model—known as RTSPA—that could serve as a useful starting place for a more comprehensive system-wide analysis. Developing and implementing a means to systematically evaluate the potential cost and effectiveness tradeoffs across aviation security countermeasures would better position TSA to achieve its stated goal of optimizing resource allocation and striking a balance of costs, effectiveness, and risk. In an environment of constrained resources and continuing threats to aviation security, producing such an analysis could assist TSA leadership in targeting its limited resources to achieve the greatest system-wide risk mitigation value for each dollar spent.

We recognize that developing these analytical methods will be a difficult undertaking that may take years to achieve. Nonetheless, as TSA improves the reliability and extent of its countermeasure effectiveness data, the agency will also improve its ability to perform system-wide cost and effectiveness tradeoff analyses. In this high threat environment, it is essential that TSA determine how to allocate its finite resources to best position the agency to detect, disrupt and deter threats to aviation security.

Recommendations for Executive Action

We are making the following two recommendations to TSA:

1. The Administrator of TSA should explore and pursue methods to assess the deterrent effect of TSA's passenger aviation security countermeasures; such an effort should identify FAMS—a countermeasure with a focus on deterring threats—as a top priority to address. (Recommendation 1)
2. The Administrator of TSA should systematically evaluate the potential cost and effectiveness tradeoffs across countermeasures, as TSA improves the reliability and extent of its information on the effectiveness of aviation security countermeasures. (Recommendation 2)

Agency Comments and Our Evaluation

We provided a draft of this report to DHS for review and comment. The department's letter is included in appendix III. In its comments, DHS generally concurred. DHS also provided technical comments, which we incorporated as appropriate.

With regard to our first recommendation that TSA explore and pursue methods to assess the deterrent effect of its passenger aviation security countermeasures, DHS concurred, noting that this may require proxy or output measures and assumptions about potential adversary choices. DHS also concurred with our second recommendation that TSA systematically evaluate the potential cost and effectiveness tradeoffs across countermeasures. In its comments, DHS stated that TSA will continue efforts to improve both its analysis of information related to security effectiveness and its cost information, leading to better informed cost-benefit decisions for individual countermeasures. To address the intent of our recommendation, TSA will need to evaluate the costs and

effectiveness of individual aviation security countermeasures and then use this information to systematically evaluate the potential cost and effectiveness tradeoffs across countermeasures. We will continue to monitor TSA's efforts in addressing these recommendations. We are sending copies of this report to the appropriate congressional committees, the Secretary of the Department of Homeland Security, and other interested parties. In addition, the report is available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at (202) 512-7141 or GroverJ@gao.gov. GAO staff who made key contributions to this report are listed in appendix IV.

A handwritten signature in black ink, reading "Jennifer Grover". The signature is fluid and cursive, with the first name "Jennifer" written in a larger, more prominent script than the last name "Grover".

Jennifer A. Grover
Director
Homeland Security and Justice Issues

List of Requesters

The Honorable Ron Johnson
Chairman
The Honorable Claire McCaskill
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Thomas R. Carper
United States Senate

The Honorable Michael McCaul
Chairman
Committee on Homeland Security
House of Representatives
The Honorable Trey Gowdy
Chairman
Committee on Oversight and Government Reform
House of Representatives
The Honorable John Katko
Chairman
Subcommittee on Transportation and Protective Security
Committee on Homeland Security
House of Representatives

Appendix I: Transportation Security Administration (TSA) Information on the Direct Costs of Selected Countermeasures

As part of this review, we analyzed TSA's fiscal year 2015 cost data for six selected aviation security countermeasures—passenger prescreening (Secure Flight), checkpoint screening, checked baggage screening, explosives detection canines, the Behavior Detection and Analysis (BDA) program, and the U.S. Federal Air Marshal Service (FAMS). We selected these six passenger aviation security countermeasures because they involved direct interaction with passengers, their belongings, or their personal information and are largely operated and funded by TSA.¹ We determined that TSA can generally identify the fiscal year 2015 direct costs to TSA of the six passenger aviation security countermeasures that we reviewed, as shown in Table 2.² TSA generally does not budget or track costs by countermeasure, but is able to identify most direct costs from their financial management system. For those passenger aviation

¹Other aviation security countermeasures not included in our review include crew vetting, federal flight deck officers, hardened cockpit doors, cargo screening, and law enforcement officers, among others.

²For purposes of this review, direct costs refers to those that can be identified as specifically benefitting one project to which TSA obligated funds in fiscal year 2015, regardless of the fiscal year in which the funds were appropriated or expended, and excludes costs incurred by other federal agencies and indirect costs (i.e., costs that have been incurred for a joint objective across multiple jurisdictions and cannot be identified as benefitting a specific project). An obligation is a definite commitment that creates a legal liability of the government for the payment of goods or services ordered, received, or a legal duty on the part of the United States that could mature into a legal liability by virtue of actions of the other party beyond the control of the United States. An agency incurs an obligation, for example, when it places an order, signs a contract, awards a grant, purchases services, or takes other actions that require the government to make payments to the public or from one government account to another. We took steps to assess the reliability of TSA's fiscal year 2015 obligations data and determined the data are sufficiently reliable for the purposes of conveying the general magnitude of costs.

**Appendix I: Transportation Security
Administration (TSA) Information on the Direct
Costs of Selected Countermeasures**

security countermeasures that align with TSA's budget categories, such as FAMS and passenger prescreening, TSA can run a single report to obtain the direct cost information.³ However, for those countermeasures that do not align with TSA's budget categories, such as checkpoint screening and checked baggage screening, TSA is able to run multiple reports and use estimation based on their staffing model to estimate the direct costs.

Table 2: Direct Cost of Selected Transportation Security Administration (TSA) Passenger Aviation Security Countermeasures in Fiscal Year 2015

TSA passenger aviation security countermeasures	Description	Fiscal year 2015 direct cost (in millions)
Passenger prescreening (Secure Flight)	TSA matches information from passengers—such as name, date of birth, and gender—against watch lists maintained by the federal government. Passengers matched to watch lists are subject to enhanced screening at the checkpoint or are not permitted to board the aircraft.	\$99.2
Checkpoint screening	TSA inspects airline passengers and their accessible baggage for prohibited and other potentially dangerous items. This includes Transportation Security Officers (TSO) checking identification documents and boarding passes, conducting pat downs, searching accessible property, and operating technology including walk-through metal detectors, X-ray machines, advanced imaging technology machines, and explosives detection equipment, among other things.	\$2,294.2 ^{a,b}
Checked baggage screening	TSA inspects airline passengers' non-accessible baggage and property for unauthorized or prohibited items through the use of explosives detection equipment.	\$1,331.5 ^{a,b}
Canines	TSA uses canine teams—a canine paired with a handler—to deter and detect explosive devices in U.S. transportation systems.	\$119.3 ^{a,c}
Behavior Detection and Analysis Program	Behavior detection officers identify persons who may pose a threat to aviation security through the observation of certain behavioral indicators—behaviors indicative of stress, fear, or deception.	\$189.4 ^a
U.S. Federal Air Marshal Service (FAMS)	FAMS deploys air marshals on flights to protect U.S. air carriers, airports, passengers, and crews.	\$800.6 ^d
Total		\$4,834.3

Source: GAO analysis of TSA information. | GAO-17-794

Notes: Costs in this table represent funds TSA obligated in fiscal year 2015, regardless of the fiscal year in which the funds were appropriated or expended. We did not include costs incurred by other federal agencies. An obligation is a definite commitment that creates a legal liability of the government for the payment of goods or services ordered, received, or a legal duty on the part of the United States that could mature into a legal liability by virtue of actions of the other party beyond the control of the United States. Direct costs are costs that can be identified as specifically benefitting one project, whereas indirect costs are costs that have been incurred for a joint objective across multiple jurisdictions and cannot be identified as benefitting a specific project. According to TSA officials, the

³TSA uses the term budget category (or "Program, Project, Activity") to generally refer to the programmatic units by which TSA organizes its budget.

**Appendix I: Transportation Security
Administration (TSA) Information on the Direct
Costs of Selected Countermeasures**

costs in this table generally exclude indirect costs such as headquarters administration, hiring and human resource costs, non-specific information technology functions, rent, and research and development because TSA does not allocate such indirect costs among TSA programs. TSA officials noted three exceptions to this. The cost of passenger prescreening includes indirect costs such as rent, utilities, and building security; the cost of FAMS captures human resources, management personnel, and office space costs; and the cost of checkpoint and checked baggage screening include the program management and operation costs associated with TSA's screening technology programs. In addition, TSA officials noted that with the exception of TSO and FAMS workers compensation costs, non-salary-related personnel costs, such as unemployment and transit benefits are not included in the cost figures because TSA does not split these expenses by program.

^aThe Screening Partnership Program (SPP), established by TSA in 2004, allows commercial (i.e., TSA-regulated) airports an opportunity to apply to TSA to have the screening of passengers and property performed by TSA-approved qualified private-screening contractors. See 49 U.S.C. § 44920. At SPP airports, TSA continues to be responsible for overseeing screening operations, and the contractors must adhere to TSA's security standards, procedures, and requirements. Throughout this report, any reference to TSOs is meant to include screeners employed by SPP contractors unless otherwise noted. According to TSA officials, TSA pays for screening costs at SPP airports but, because the costs are paid through a contract, TSA generally does not track all costs at SPP airports at the same level of detail as for non-SPP airports. As a result, in the table above the costs of BDO staff at SPP airports are not included in the behavior detection program cost. Rather, these costs are included in the checkpoint and checked baggage screening costs. According to TSA officials, at the end of fiscal year 2015, 21 of 437 commercial airports in the United States participated in the SPP program.

^bThe direct costs for checkpoint and checked baggage screening include the costs of both people—TSOs including screeners employed by SPP contractors—and equipment. TSA officials explained that TSA does not track the portions of TSO labor costs associated with checkpoint screening and checked baggage screening because they've determined that the administrative burden of collecting this data outweighed the benefit. Rather, TSA estimates that 75 percent of total TSO time is spent at checkpoint screening and 25 percent is spent at checked baggage screening and uses these figures in its TSO staffing allocation model as well as to estimate the division of total TSO costs between checkpoint and checked baggage screening. Further, TSA officials explained that because training costs are large contract costs that support a variety of workforce personnel, TSA does not track the portions of overall training costs associated with checkpoint and checked baggage, so training costs are generally not included in the figures presented.

^cAccording to TSA officials, during fiscal year 2015, TSA moved to a multimodal canine model—in which canine teams work in multiple environments beyond the passenger aviation environment—and merged all costs associated with canine teams into a single accounting category. As a result, TSA officials report that this cost includes some costs of canines that are deployed in non-aviation environments, such as mass transit.

^dTSA officials explained that the cost of FAMS's scheduling system is excluded because TSA does not isolate that cost from other TSA information technology costs.

Appendix II: Fiscal Year 2015 Effectiveness Data for Selected Passenger Aviation Security Countermeasures

The Transportation Security Administration (TSA) collected fiscal year 2015 data on the effectiveness of four of the six countermeasures we selected—passenger prescreening, checkpoint screening, checked baggage screening, and explosives detection canines.¹ These data show mixed results with some data indicating TSA countermeasure effectiveness and other data highlighting vulnerabilities. Below, we describe what TSA knows about the fiscal year 2015 effectiveness of these four countermeasures in detecting or disrupting threats to passenger aviation security.

Overview of Passenger Prescreening

TSA uses its Secure Flight prescreening program to match passenger information against federal government watch lists and other information to assign each passenger to one of three risk categories—high risk, low risk, or unknown risk—that either corresponds to the level of screening they will experience at the checkpoint or may deny them an opportunity to board the aircraft. Since TSA began implementing Secure Flight in 2009, the passenger prescreening program has changed from a program that identifies passengers as high risk solely by matching them against federal government watch lists—for example, the No Fly List, comprised of individuals who should be precluded from boarding an aircraft, and the Selectee List, comprised of individuals who should receive enhanced screening at the passenger security checkpoint—to one that uses additional lists and risk-based criteria to assign passengers to a risk category.² Specifically, Secure Flight now identifies passengers as high

¹In fiscal year 2015, TSA did not collect data on the security effectiveness of the Behavior Detection and Analysis program or the U.S. Federal Air Marshal Service.

²The No Fly and Selectee Lists are subsets of the Terrorist Screening Database—the U.S. government's consolidated watch list of known or suspected terrorists.

risk if they are matched to watch lists of known or suspected terrorists or other lists developed using certain high-risk criteria and as low risk if they are deemed eligible for expedited screening through TSA Pre✓™—a 2011 initiative to preapprove passengers for expedited screening—or through the application of low-risk rules.³ Secure Flight identifies passengers as unknown risk if they do not fall within the other two risk categories.

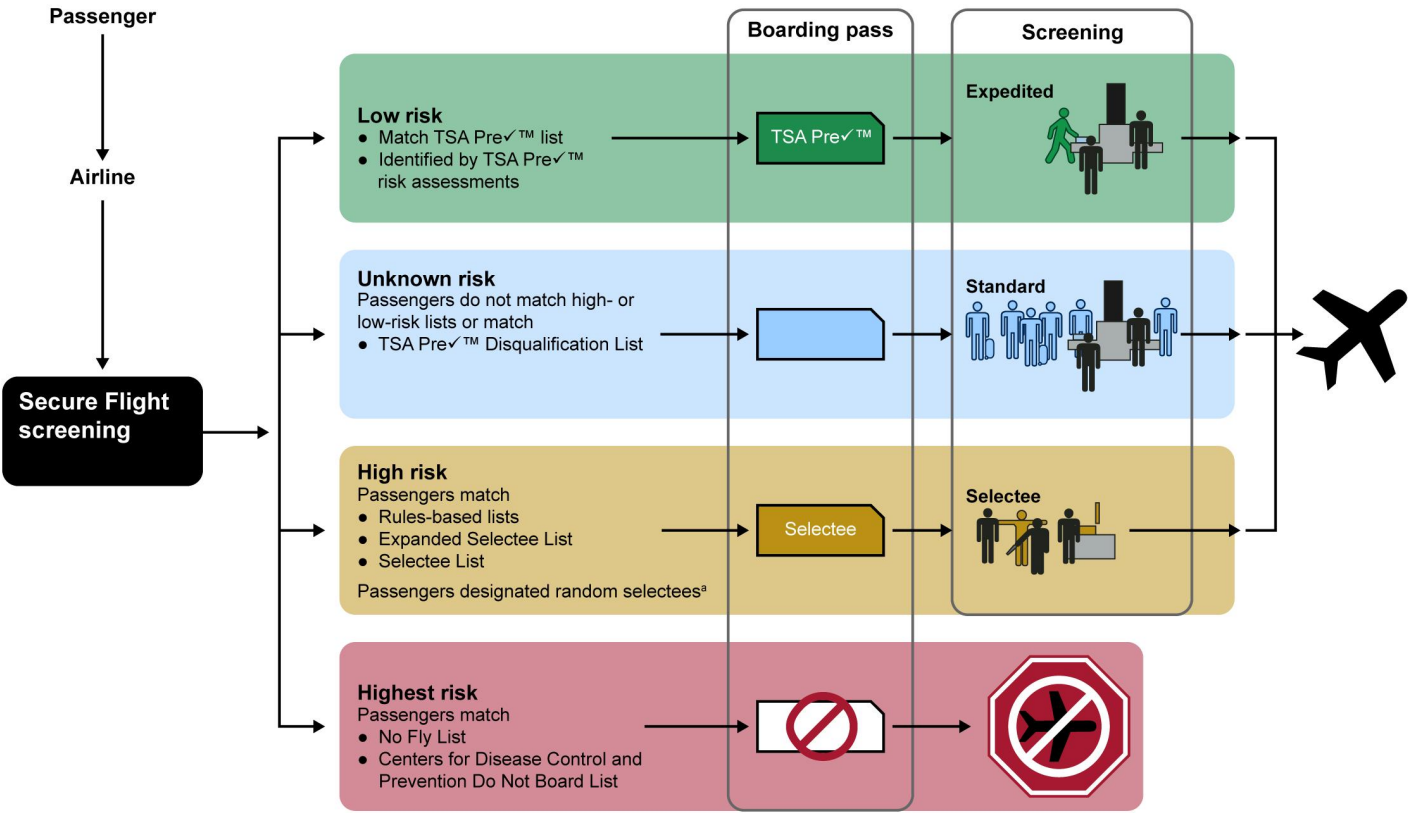
To separate passengers into these risk categories, TSA utilizes lists in addition to the No Fly and Selectee Lists, and TSA has adapted the Secure Flight system to perform risk assessments, a system functionality that is distinct from both watch list matching and matching against lists of known travelers.⁴ At airport checkpoints, those passengers identified as high risk receive enhanced screening, passengers identified as low risk are eligible for expedited screening, and passengers identified as unknown risk generally receive standard screening. Passengers matched to the No Fly List or the Centers for Disease Control and Prevention's Do Not Board List—a list which includes individuals who pose a significant health risk to other travelers and are not allowed to fly—are considered highest risk, and thus are not to receive boarding passes, and should not

³In 2010, TSA began using rules-based lists to identify and designate for enhanced screening passengers who may represent unknown threats. TSA develops these lists by comparing U.S. Customs and Border Protection international passenger data to law enforcement, intelligence, and other enforcement data using risk-based targeting scenarios and assessments. In July 2012, TSA also began screening against a TSA Pre✓™ Disqualification Protocol List, a watch list created and maintained by TSA that includes individuals who, based upon their involvement in violations of security regulations of sufficient severity or frequency (e.g., bringing a loaded firearm to the checkpoint), are disqualified from receiving expedited screening for some period of time or permanently.

⁴For example, in April 2011, TSA began conducting watch list matching against an Expanded Selectee List in order to designate more passengers who are known or suspected terrorists as selectees for enhanced screening. In general, this list includes all records in the Terrorist Screening Database with a full name (first name and surname) and full date of birth but that are not included on the No Fly or Selectee Lists. To further increase the number of passengers identified as low risk (and therefore TSA Pre✓™ eligible), TSA also adapted the Secure Flight system to begin assigning passengers risk scores based upon their travel-related data, for the purpose of identifying them as low risk for a specific flight.

be allowed entry into the sterile area.⁵ Figure 3 illustrates this passenger prescreening process.

Figure 3: Transportation Security Administration (TSA) Passenger Prescreening Process



Source: GAO analysis of TSA information. | GAO-17-794

^aThese individuals are identified for enhanced screening at random, not because they are included on government watch lists.

The Effectiveness of Passenger Prescreening in Fiscal Year 2015

TSA officials reported that the percentage of passengers vetted and the number of high-risk passengers identified by Secure Flight demonstrate

⁵See 49 C.F.R. § 1540.5 (defining the sterile area of the airport as, in general, an area of an airport that provides passengers access to boarding aircraft and to which access is controlled through the screening of persons and property).

the effectiveness of this passenger prescreening program. Specifically, TSA data indicate that in fiscal year 2015, Secure Flight vetted 100 percent of the over 816 million records submitted for passengers who flew into, out of, over, or within the United States, and on U.S.-flagged aircraft operating internationally point-to-point.⁶ Of these, TSA identified 15,383 (0.002 percent of passenger records vetted) as confirmed matches to watch lists. Specifically, in fiscal year 2015, TSA identified 9,639 passengers as expanded selectees, 5,019 passengers on the Selectee List, and 725 passengers on the No Fly List.⁷

In September 2014, we reported that TSA collects and regularly reviews data on the number of passengers identified by the Secure Flight system as potential matches to the No Fly, Selectee, and Expanded Selectee Lists.⁸ However, we found that TSA did not measure the extent to which Secure Flight was missing passengers who were actual matches to these lists—false negatives. We recommended that TSA establish such measures. In response, in August 2016, TSA contracted with a third party to conduct an independent assessment of the effectiveness of the Secure Flight automated vetting system including whether Secure Flight identifies the matches it should (i.e., how well the system minimizes false negatives). TSA officials expect this assessment to be complete at the end of calendar year 2017.

Overview of Checkpoint Screening

TSA ensures that all individuals and accessible property are screened as part of its checkpoint screening process to deter and prevent the carriage of any unauthorized explosive, incendiary, weapon, or other prohibited

⁶A single individual who flew into, out of, over, or within the United States, or on U.S.-flagged aircraft operating internationally point-to-point multiple times in fiscal year 2015 would be counted multiple times in these data.

⁷TSA officials explained that they began manually reviewing and confirming expanded selectee matches in April 2015. Further, these Secure Flight vetting statistics do not include matches to rules-based lists TSA also uses to identify passengers who may represent unknown threats and designate them for enhanced screening. According to TSA, beginning in fiscal year 2015, Secure Flight also identified passengers for enhanced screening using rules-based lists. In fiscal year 2015, Secure Flight also matched 41 passengers to the Centers for Disease Control and Prevention's Do Not Board List which, like the No Fly List, requires that air carriers not issue the passenger a boarding pass.

⁸GAO, *Secure Flight: TSA Should Take Additional Steps to Determine Program Effectiveness*, [GAO-14-531](#) (Washington, D.C.: Sept. 9, 2014).

items on board an aircraft or into the airport sterile area—in general, an area of an airport that provides passengers access to boarding aircraft and to which access is controlled through the screening of persons and property.⁹ Ordinarily, screening of accessible property at the screening checkpoint begins when an individual places accessible property on the X-ray conveyor belt or hands accessible property to a Transportation Security Officer (TSO).¹⁰ As shown in figure 4, TSOs then review images of the property running through the X-ray machine and look for signs of prohibited items.¹¹ If a TSO identifies a potential prohibited item, the accessible property will be manually inspected and screened with an explosives trace detection (ETD) machine to identify any traces of explosives material. The passengers themselves are typically screened via a walk-through metal detector or an advanced imaging technology (AIT) machine—often referred to as a full-body scanner—and passengers generally have the option to request screening by a pat down if they do not wish to be screened by these technologies. Passengers will also be subject to a pat down if they are screened by a walk through metal

⁹See 49 C.F.R. § 1540.5 (defining “sterile area”). TSOs must deny passage beyond the screening checkpoint to any individual or property that has not been screened or inspected in accordance with passenger screening standard operating procedures. See 49 C.F.R. § 1540.107(a); see also 49 U.S.C. § 44902 and 49 C.F.R. §§ 1544.201(c) and 1546.201(c) (requiring, in general, that U.S. and foreign-flagged air carriers refuse to transport any individual who does not consent to a search or inspection of his or her person and property).

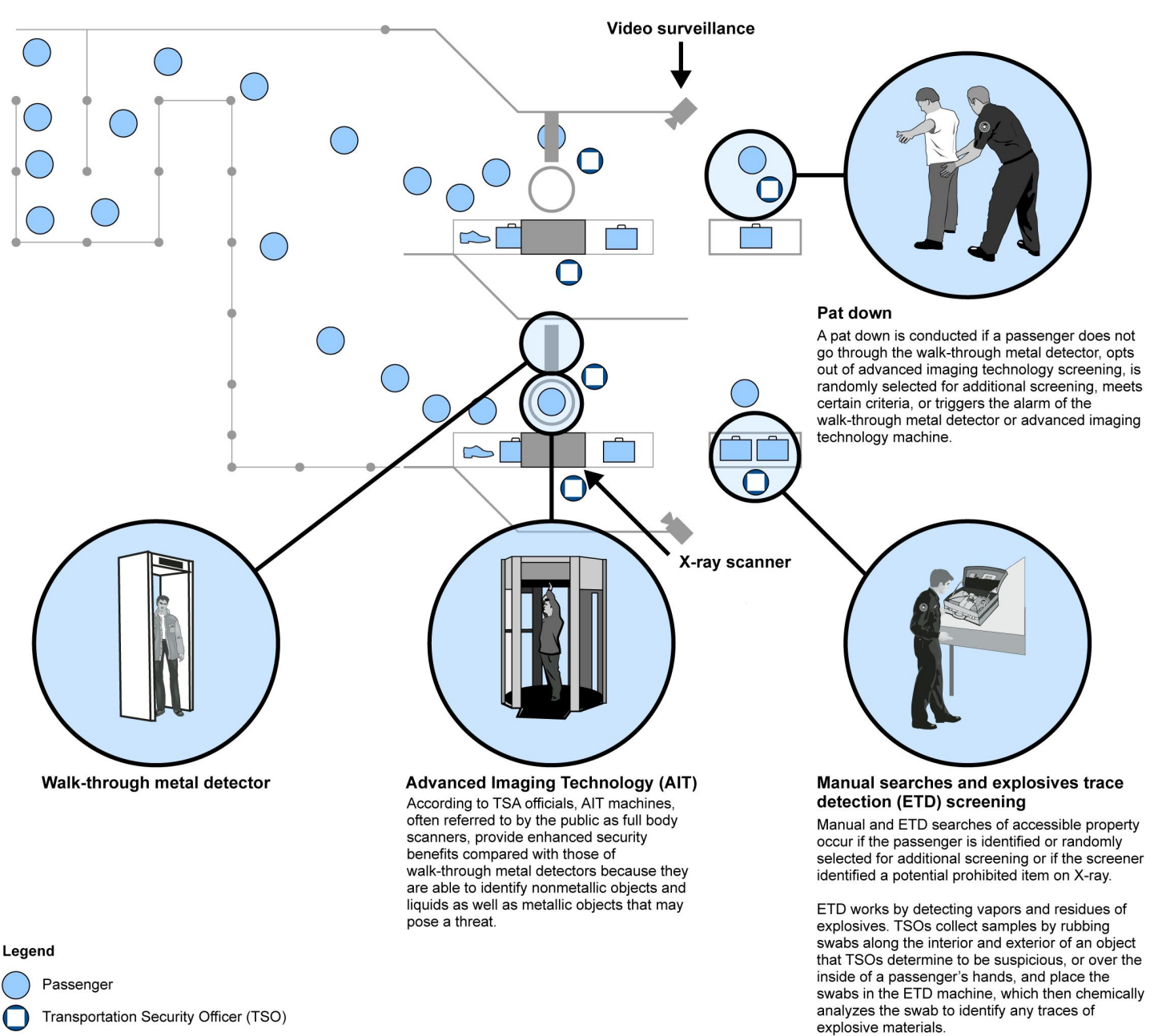
¹⁰The Screening Partnership Program (SPP), established by TSA in 2004, allows commercial (i.e., TSA-regulated) airports an opportunity to apply to TSA to have the screening of passengers and property performed by TSA-approved qualified private-screening contractors. See 49 U.S.C. § 44920. At SPP airports, TSA continues to be responsible for overseeing screening operations, and the contractors must adhere to TSA’s security standards, procedures, and requirements. According to TSA officials, at the end of fiscal year 2015, 21 of the 437 commercial airports in the United States participated in the SPP program. Throughout this report when we refer to TSOs, we also mean screeners employed by SPP contractors, unless otherwise noted.

¹¹To provide passengers with guidance on the types of items TSA policy prohibits from being carried onto an aircraft, TSA maintains a Prohibited Items List that lists items passengers may not carry into the sterile area or onboard an aircraft, which is available through TSA’s website at <https://www.tsa.gov/travel/security-screening/prohibited-items>. The list is not exhaustive, but rather includes examples and categories of items that are prohibited, and TSOs may use their discretion to prohibit items they deem could pose a threat to transportation security.

detector or the AIT and the equipment alarms (in order to resolve the alarm).¹²

¹²Passengers and their accessible property may also be randomly selected for additional screening, which commonly includes a pat down for the passenger and a manual inspection or ETD screening of their accessible property.

Figure 4: Transportation Security Administration’s (TSA) Passenger Screening Checkpoint



Source: GAO analysis of TSA information; Art Explosion (clip art). | GAO-17-794

TSOs use several screening technologies in order to screen passengers and carry-on bags for prohibited items. For more information on the

specific screening technologies deployed at the checkpoint in fiscal year 2015, see Table 3.

Table 3: Summary of Transportation Security Administration (TSA) Checkpoint Screening Technologies Deployed in Fiscal Year 2015

Technology	Description	Number of Machines	Number of Airports ^a
Advanced Imaging Technology (AIT)	TSA uses advanced imaging technology to screen passengers for potential threats. This technology detects a range of metallic and nonmetallic threats on passengers and highlights the location of potential threats on a generic passenger outline for further assessment by Transportation Security Officers (TSO).	780	190
Walk-Through Metal Detector	TSA uses walk-through metal detectors to screen passengers for potential threats.	1,435	437
Advanced Technology X-ray	TSA uses advanced technology X-ray machines to screen passengers' carry-on baggage. These machines use detection algorithm software to identify potential threats such as explosives in carry-on baggage and provide a horizontal and vertical image of each screened item to the TSO.	2,186	437
Bottled Liquid Scanner	TSA uses bottled liquid scanners to differentiate dangerous from nonthreatening liquids carried by passengers through checkpoint screening.	1,585	434 ^b
Explosives Trace Detection Machine	TSA uses explosives trace detection machines to detect explosive compounds on airline passengers as well as on their carry-on and checked baggage.	2,624	437

Source: GAO analysis of TSA data. | GAO-17-794

^aAccording to TSA, there were a total of 437 commercial (i.e. TSA-regulated) airports in the United States at the end of fiscal year 2015. TSA classifies these airports into one of five categories (X, I, II, III, and IV) based on various factors, such as the number of take-offs and landings annually, the extent of passenger screening at the airport, and other security considerations. In general, Category X airports have the largest number of passenger boardings and Category IV airports have the smallest.

^bAccording to TSA, the airports that did not have a bottled liquid scanner were Category IV airports that had not yet received their allocation of one bottled liquid scanner by the end of fiscal year 2015, but as of March 2017, all airports are now equipped with this technology.

The Effectiveness of Checkpoint Screening in Fiscal Year 2015

In fiscal year 2015, TSA collected data on the effectiveness of checkpoint screening by testing TSOs, screening technology (e.g., the AIT and X-ray), and the checkpoint screening system as a whole (i.e., the combination of TSOs and technology).¹³

¹³As noted earlier, throughout this report when we refer to TSOs, we also mean screeners employed by SPP contractors, unless otherwise noted.

Checkpoint Screening TSOs

TSA collected fiscal year 2015 data on the effectiveness of its TSO workforce in detecting or disrupting threats to aviation security at the checkpoint in three ways: (1) annual proficiency review (APR) of TSOs, (2) threat-image projection (TIP) testing, and (3) Aviation Screening Assessment Program (ASAP) Advantage covert tests.¹⁴

Annual Proficiency Reviews. APRs evaluate TSOs' skill in performing the various checkpoint and checked baggage screening functions and all TSOs must successfully complete the required APR component tests related to their job function on an annual basis as a condition of employment with TSA in their capacity as a screener.¹⁵ Components of the APR focused on checkpoint screening specifically included tests that evaluate TSOs' ability to identify prohibited items on an X-ray machine and tests that evaluate whether TSOs can perform various practical skills such as pat downs, bag searches, and use of explosive trace detection technology.¹⁶

¹⁴TSA officials estimate that 75 percent of all TSO time is spent on checkpoint screening. In fiscal year 2015, this would be the full-time equivalent of approximately 34,000 of TSA's roughly 45,000 TSOs conducting checkpoint screening, though individual TSOs often divide their time between checkpoint and checked baggage screening. TSA officials explained that they do not track the portions of TSO labor associated with checkpoint screening and checked baggage screening operations. Rather, TSA estimates that 75 percent of total TSO time is spent at checkpoint screening and 25 percent is spent at checked baggage screening and uses these figures in its TSO staffing allocation model.

¹⁵In accordance with ATSA, TSOs are required to pass the Annual Proficiency Review to continue to remain employed in that capacity. See 49 U.S.C. § 44935(f)(5). If a TSO does not pass one of the components of the APR after two or, in some cases, three attempts, they are subject to removal from their position. Beginning in 2015, TSA changed its APR testing cycle from fiscal year to calendar year. As a result, we present calendar year 2015 APR data in this report.

¹⁶The APR component tests that an individual TSO must take depend on whether that TSO is certified to perform checkpoint screening, checked baggage screening, or has dual certification to perform both functions. Portions of the APR are computer-based X-ray image tests done in a non-operational setting away from the active checkpoints while the remaining tests are skills demonstrations performed in a realistic, but inactive, screening environment such as an unused screening lane.

In calendar year 2015, TSA conducted roughly 150,000 APR component tests focused on checkpoint screening.¹⁷ Table 4 provides descriptions of these component tests.¹⁸

Table 4: Description of Annual Proficiency Review (APR) Component Tests for Checkpoint Screening in Calendar Year 2015

APR Component Test	Description
Image Mastery Assessment	This is an X-ray interpretation assessment to determine whether officers can detect threat items in a passenger's carry-on bag at the passenger screening checkpoint.
Standard Pat Down ^a	This is an assessment to ensure officers know how to properly conduct a standard pat down of passengers at the screening checkpoint as required by the screening Standard Operating Procedures (SOP).
Screening of Individuals with Disabilities	This is an assessment to ensure officers know how to properly screen certain individuals with disabilities (i.e., passengers in wheelchairs who are unable to stand) in accordance with the screening SOP.
Physical Bag Search Passengers	This is a physical bag search assessment for passengers' carry-on baggage.
Explosives Trace Detection Assessment for Passengers	This is an explosives trace detection assessment for the passenger checkpoint. The assessment ensures officers know what items to check for explosives trace material as required by the SOP.

Source: GAO analysis of Transportation Security Administration data. | GAO-17-794

^aDuring fiscal year 2015, TSA's standard operating procedures required a standard pat-down of passengers when, for example, an individual opted out of advanced imaging technology screening or to resolve screening technology alarms, among other reasons.

Threat Image Projection (TIP) Testing. TSA's TIP testing system displays fictional threat items, such as guns or explosives, onto X-ray images of actual passengers' carry-on bags to test TSOs' ability to

¹⁷This represents the number of first-time tests conducted for specific APR component tests required for the nearly 18,000 TSOs certified to perform checkpoint screening only at both SPP and non-SPP airports during calendar year 2015. TSOs certified to perform checked baggage screening only—roughly 4,200 TSOs in calendar year 2015— or have dual certification to perform both screening functions—approximately 14,400 TSOs in calendar year 2015—take similar, but different APR component tests. For instance, a TSO certified to perform checkpoint screening only must take the ETD Assessment for Passengers component test whereas a TSO dual certified to perform both passenger screening and checked baggage screening would take the ETD Assessment for Checked Baggage component test.

¹⁸First-time pass rates for these component tests have been designated as sensitive security information and thus cannot be included in a public report.

identify prohibited items in a live operational environment. TSOs operating the X-ray machine at the checkpoint are monitored to see if they positively identify the threat image and call for the bag to be searched. TSA officials report that they use TIP images on a daily basis to monitor TSOs' ability to identify prohibited items, aid in keeping them focused and attentive, and keep their skills sharp in identifying items they do not routinely see.¹⁹ TSA requires airport personnel to conduct TIP tests and upload monthly results data into TSA's national database.

In September 2016, we reported that TSA's TIP data from fiscal year 2009 through 2014 was incomplete as TSA could not provide TIP scores for every airport during this period.²⁰ Specifically, during fiscal year 2013, nearly 14 percent of airports failed to report any TIP data. TSA officials also acknowledged that, in addition to the airports that did not report any TIP data for a year or more at a time, other airports may have reported only partial TIP results data during this same time frame. We recommended that TSA officials at individual airports submit complete TIP results to the TSA national database as required and, further, that TSA analyze national TIP data for trends that could inform training needs and improve future training and TSO performance assessments. TSA concurred with our recommendations and is taking steps to address them. Specifically, a new TIP Operations Directive was implemented in October 2016 to disseminate procedures for performance data collection and submission to improve TIP data. According to agency officials, the number of non-compliant airports decreased during fiscal year 2016. However, since these improvements occurred during fiscal years 2016 and 2017, fiscal year 2015 TIP data remained incomplete and unreliable for the purposes of assessing TSO's effectiveness at identifying TIP images. Therefore, we do not present fiscal year 2015 TIP test results in this report.

¹⁹According to TSA policy, Federal Security Directors must monitor TIP results monthly and if a TSO identifies less than a certain percent of TIP images accurately in a month, then the TSO is required to attend remedial training. Federal Security Directors are TSA officials responsible for overseeing TSA security activities, including passenger and checked baggage for screening, at one or more of the nation's commercial airports. See 49 U.S.C. § 44933.

²⁰See GAO, *Aviation Security: TSA Should Ensure Testing Data Are Complete and Fully Used to Improve Screener Training and Operations*, [GAO-16-704](#) (Washington, D.C.: September 2016).

Aviation Screening Assessment Program (ASAP) Advantage

Testing. To measure TSO performance nationwide in fiscal year 2015, TSA used standardized ASAP covert tests conducted by local TSA testers at each airport. ASAP tests focused on checkpoint screening were designed to assess the operational effectiveness of TSOs in identifying and preventing prohibited items, such as knives, guns, or simulated improvised explosive devices, from being taken through the checkpoint by testers.²¹ In fiscal year 2015, TSA conducted 5,213 ASAP covert tests on checkpoint screening at 170 airports.²²

TSA hired a contractor in fiscal year 2015 to independently conduct ASAP standard scenario tests at 40 airports to assess the validity of TSA testing results at those airports.²³ When comparing the contractor's results to the local TSA testers' results, TSA found moderate to significant differences in the two sets of test results for most of the 40 airports. According to TSA officials, TSOs generally performed more poorly in the ASAP tests conducted by the independent contractor personnel when compared to the ASAP testing conducted by the local TSA personnel—indicating that pass rates for tests conducted by local TSA personnel were likely showing a higher level of TSO performance than was actually the case. TSA officials reported that the differences in test results have led them to question the extent to which the ASAP tests accurately measure TSO performance. As a result, we do not present the fiscal year 2015 ASAP test results in this report.

²¹ ASAP tests are designed to trigger screening technology to alarm in order to specifically test TSOs' ability to follow standard operating procedures and resolve this alarm. Therefore, ASAP tests are not designed to test the effectiveness of the screening technology itself.

²² In fiscal year 2015, TSA conducted two types of ASAP covert tests—targeted scenarios and standard scenarios. Targeted scenarios are assessments conducted at the discretion of federal security directors and used at the individual airport level to provide additional TSO training. Standard scenarios are mandatory and airports must conduct the assigned assessments. TSA uses the data generated from these standardized scenarios to assess ASAP testing results at the national level. In fiscal year 2015, TSA conducted ASAP tests at both SPP and non-SPP airports.

²³ According to TSA, the goals of the independent covert testing done by the contractor were to (1) establish a baseline of expected TSO performance, (2) assess the ASAP program, (3) validate the accuracy of historical ASAP data, and (4) capture and record sources of officer failure to follow procedures and detect threats and identify the root causes of the failures to follow procedure.

To address this validity issue, in April 2016, TSA officials reported that they began using both headquarters-based covert testing teams composed of headquarters-based TSA employees and field-based covert testing teams composed of local testers in both the checkpoint and checked baggage screening environments at all airports.²⁴ Both headquarters-based and field-based teams conduct the same scenario-based covert tests that were previously conducted as part of ASAP testing. TSA officials stated that comparing the results of these separate tests has provided TSA with a way to gauge the validity of its test results.²⁵

Checkpoint Screening Technology

TSA officials reported that the effectiveness of checkpoint screening technology in fiscal year 2015 is best described by each type of machine's detection standard—the specified rate of detection each technology is required to achieve in identifying explosives or prohibited items.²⁶ Specific details about TSA's detection standards are omitted because the information is classified. Prior to acquiring and deploying a potential new screening technology, TSA conducts testing to evaluate

²⁴According to TSA officials, TSA conducts roughly 8,000 field-based covert tests and 4,000 headquarters-based covert tests each year. For example, TSA officials reported conducting field-based covert tests at about half of all commercial airports in the United States during fiscal year 2015. These included all Category X, I, and II airports, roughly 50 percent of Category III airports, and 5 percent of Category IV airports. For headquarters-based testing, which began in April 2016, TSA officials reported conducting covert tests at approximately 20 percent of airports during fiscal year 2016. These included all Category X and I airports and 12 percent of Category II airports. TSA did not conduct headquarters-based covert testing at Category III and IV airports. These operational tests have replaced the ASAP Advantage program.

²⁵Additionally, in 2016, as part of the headquarters-based and field-based testing process, TSA began using the new Task Process Factors tool, which collects additional data on the type of threat being tested, the environmental factors present at the time of the test, and the root causes of any failures, among other things. According to TSA officials, the Task Process Factors tool allows TSA to quickly and easily disseminate standardized covert testing data that are essential for understanding weaknesses and vulnerabilities in TSA's screening system to TSA leadership as well as airports across the country. Among other uses, these data can be used to better inform TSA's corrective actions and training priorities.

²⁶TSA also tests the effectiveness of its screening technology through its Office of Inspection (OOI) Red Team Covert Testing. However, as discussed later in this report, these tests are not designed to specifically test the screening technology, but to test the checkpoint screening system as a whole.

whether potential technologies can effectively achieve the detection standards required by TSA, among other things.²⁷

Once technology is deployed in the airport environment, TSA policy requires at least daily calibration testing of each individual piece of technology deployed at the checkpoint—AIT machines, walk through metal detectors, ETDs, and X-ray machines, among others—to ensure the technology is functioning properly and able to achieve the required detection standards.²⁸ For example, each day when the screening checkpoint opens, TSOs must ensure that AIT machines successfully complete an image quality verification, a calibration test, and an operational test process before they are cleared for screening operations.²⁹ TSA policy requires that TSOs record the results of these

²⁷This testing is performed in three phases: qualification and certification testing at the Transportation Security Laboratory, qualification testing at the TSA Systems Integration Facility (TSIF), and operational testing at selected airports. The qualification testing is conducted at the TSIF, located in Arlington, Virginia. Testing at the TSIF is designed to verify system performance against defined functional requirements, such as system capacities, human factors, physical characteristics, user safety, and system reliability, availability, and maintainability. All countermeasures must pass qualification testing at TSIF and undergo an operational test readiness review before they can proceed to operational testing at select airports. In the course of this review we visited the TSIF to observe how TSA tests screening technology prior to deployment. Once a technology is determined to be operationally effective, TSA places this technology on its qualified products list—a register of technologies that have been examined, tested, and have satisfied all qualification requirements—after which it can be acquired and deployed at airports.

²⁸In December 2013, we reported that TSA was not capturing data on false alarm rates for certain AIT machines deployed to screening checkpoints, including false positives—when an AIT alarms but should not have—and false negatives—when an AIT should have alarmed but did not. We reported that data on AIT false alarm rates could be used to analyze and monitor the potential impacts of these false alarms on TSA's operational costs at the checkpoint. We recommended that TSA establish a process to capture operational data on the results of TSOs' secondary screening of passengers to resolve technology alarms in order to determine the extent to which AIT false alarm rates affect TSA's operational costs. While TSA initially concurred with our recommendation, TSA officials subsequently determined that implementing it would not be feasible due to difficulties in collecting accurate data in a live airport environment. As a result, we closed this recommendation as not implemented. See GAO, *Advanced Imaging Technology: TSA Needs Additional Information before Procuring Next Generation Systems*, [GAO-14-357](#) (Washington, D.C.: March 31, 2014).

²⁹Additional calibration and operational tests are conducted for other reasons, such as when a piece of screening technology is powered on after a power outage or undergoes routine maintenance. TSA personnel also conduct equipment tests whenever they have reason to believe the system is not functioning properly.

tests in logbooks and, further, that any screening equipment that does not pass daily testing be immediately taken out of service.

TSA's Checkpoint Screening System as a Whole

In fiscal year 2015, TSA collected data on the effectiveness of its checkpoint screening system as a whole—including both screening technology and TSO performance—through Red Team covert testing conducted by TSA's Office of Inspection (OOI).³⁰ In fiscal year 2015, TSA conducted numerous Red Team covert tests on checkpoint screening at a random sample of U.S. airports.³¹ During passenger checkpoint testing, each team of inspectors carries threat items, such as simulated explosive devices, through the passenger checkpoint. If the TSO identifies the threat item during screening, the inspector identifies him or herself to the TSO and the test is considered a pass. If the TSO does not identify the threat item, the inspector proceeds to the sterile area of the airport and the test is considered a failure. According to TSA, these tests are designed to approximate techniques that terrorists may use in order to identify vulnerabilities in the people, processes, and technologies that comprise the aviation security system. In addition to OOI's Red Team testing, in fiscal year 2015 the Department of Homeland Security (DHS) Office of Inspector General (OIG) also conducted covert tests of certain TSA checkpoint operations at 8 U.S. airports that use AIT machines to screen passengers. According to the DHS OIG, the objective of the tests was to determine the effectiveness of TSA's AIT, automated target recognition software (which displays a box around anomalies on a generic outline of a body), and checkpoint screener performance in identifying and resolving anomalies and potential security threats at airport checkpoints. The results of both the OOI Red Team and the DHS OIG's covert tests are omitted because the information is classified.

³⁰TSA officials reported that Red Team tests are developed and deployed based upon current intelligence of threats against transportation systems.

³¹Results of OOI's Red Team covert tests provide insights about the effectiveness of checkpoint and checked baggage screening, but observations from these airports are not generalizable to all TSA-regulated airports in the United States. OOI officials report that in fiscal year 2015 their Red Team testing included both SPP airports and non-SPP airports.

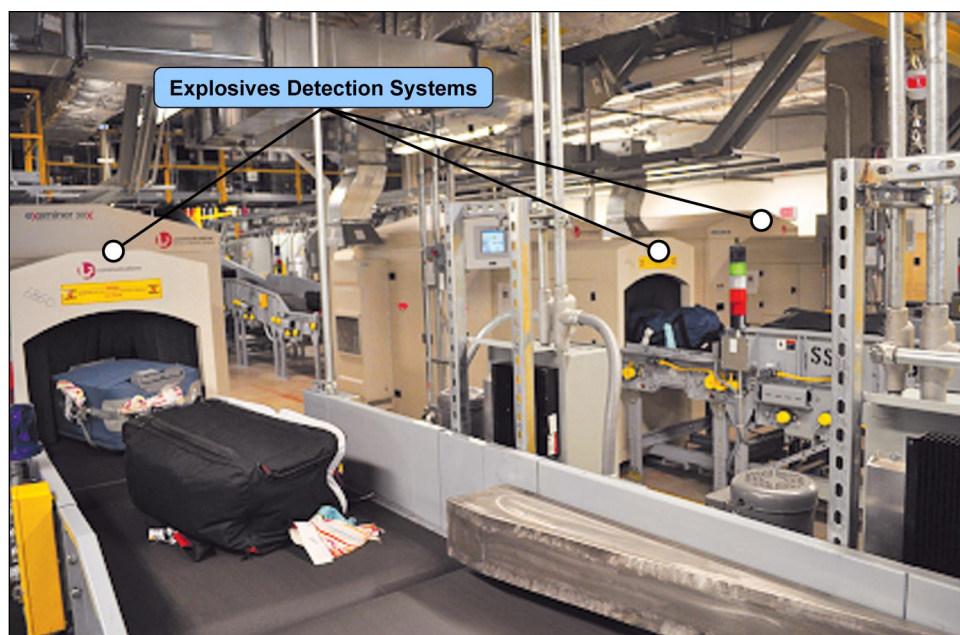
Overview of Checked Baggage Screening

TSA inspects passengers' checked baggage to deter, detect, and prevent the transport of any unauthorized explosive, incendiary, or weapon onboard an aircraft.³² Checked baggage screening is accomplished through the use of explosives detection systems (EDS)—which use X-rays with computed tomography technology to automatically measure the physical characteristics of objects in baggage and automatically trigger an alarm when objects that exhibit the physical characteristics of explosives are detected—and explosives trace detection (ETD) machines, in which TSOs swab baggage and use chemical analysis to manually detect traces of explosive materials' vapors and residue.³³

³²See 49 U.S.C. § 44901; 49 C.F.R. § 1540.111(c). See also 49 U.S.C. § 44902 and 49 C.F.R. § 1544.203(e) and 1546.203(b) (requiring, in general, that air carriers refuse to transport any individual's checked baggage or property if the individual does not consent to a search or inspection of that checked baggage or property).

³³At airports with EDS, EDS machines are generally employed for primary screening of checked baggage while ETD machines are used for secondary screening to help resolve questions raised by EDS screening. At airports without EDS machines, ETDs are used as the primary method for screening checked baggage.

Figure 5: A Checked Baggage Inspection Configuration That Includes Three Explosives Detection Systems



Source: GAO. | GAO-17-794

Generally, a checked baggage screening system at airports with EDS includes a three-level screening process. First, EDS machines perform automated screening. If the EDS machine determines that a checked bag requires additional screening, it sends an alarm to a TSO who performs a secondary inspection known as On-Screen Resolution by reviewing an image of the contents of the bag on a computer monitor. If the TSO cannot resolve the alarm using on-screen resolution tools and determines a physical bag search is necessary, the bag goes to the Checked Baggage Resolution Area where a TSO performs a manual inspection of the bag assisted by an ETD machine.

At the end of fiscal year 2015, TSA had 1,717 EDS machines deployed at 263 airports. At airports without EDS, which are typically smaller airports, ETD machines are the primary method for manually screening checked baggage. At the end of fiscal year 2015, TSA had 2,291 ETD machines deployed at all 437 commercial (i.e., TSA-regulated) airports for primary or secondary screening of checked baggage.

TSA officials estimate that 25 percent of total TSO time is spent on checked baggage screening, and in fiscal year 2015, this would be the

full-time equivalent of approximately 11,000 of TSA's roughly 45,000 TSOs conducting checked baggage screening.³⁴

The Effectiveness of Checked Baggage Screening in Fiscal Year 2015

In fiscal year 2015, TSA collected data on the effectiveness of its checked baggage screening by testing screening personnel (i.e., TSOs), screening technology (EDS and ETD machines), and the checked baggage screening system as a whole (i.e., the combination of TSOs and technology).

Checked Baggage Screening TSOs

In fiscal year 2015, TSA collected data on the effectiveness of its TSO workforce in detecting or disrupting threats to aviation security in the checked baggage environment through its APR evaluations and ASAP Advantage covert tests.

Annual Proficiency Reviews (APR). As discussed above, APRs evaluate TSOs' skill in performing the various checkpoint and checked baggage screening functions.³⁵ Components of the APR focused on checked baggage screening include tests that evaluate TSOs' ability to resolve EDS machine alarms using the appropriate tools and practical skills such as bag searches and the use of ETD technology.³⁶

³⁴As noted above, TSA officials explained that they do not track the portions of TSO labor associated with checkpoint screening and checked baggage screening operations because they've determined that the administrative burden of collecting this data outweighed the benefit. Rather, TSA estimates that 75 percent of total TSO time is spent at checkpoint screening and 25 percent is spent at checked baggage screening.

³⁵Beginning in 2015, TSA changed its APR testing cycle from fiscal year to calendar year. As a result, we present calendar year 2015 APR data in this report. In accordance with ATSA, TSOs are required to pass the Annual Proficiency Review to continue to remain employed in that capacity. See 49 U.S.C. § 44935(f)(5).

³⁶The APR components that an individual TSO must take are dependent on whether that TSO is certified to perform checkpoint screening, checked baggage screening, or has dual certification to perform both functions. Portions of the APR are computer-based X-ray image tests done in a non-operational setting away from the active checkpoints while the remaining tests are skills demonstrations performed in a realistic, but inactive, screening environment such as an unused screening lane.

In calendar year 2015, TSA conducted nearly 35,000 APR component tests specific to the checked baggage screening environment.³⁷ Table 5 provides descriptions of these component tests.³⁸

Table 5: Description of Annual Proficiency Review (APR) Component Tests for Checked Baggage Screening in Calendar Year 2015

APR Component Test	Description
On-Screen Alarm Resolution Protocol Annual Assessment	This is an assessment to determine if Transportation Security Officers can properly follow an alarm resolution flow chart and determine if checked baggage contains a threat item.
Physical Bag Search for Checked Baggage	This is a physical bag search assessment for checked baggage.
Explosives Trace Detection Assessment for Checked Baggage	This is an explosives trace detection assessment for checked baggage to determine if officers know what items to check for explosive trace material as required by the screening standard operating procedure.

Source: GAO analysis of Transportation Security Administration data. | GAO-17-794

Note: The test data presented in this table include the results of tests conducted at both Screening Partnership Program (SPP) and non-SPP airports.

Aviation Screening Assessment Program (ASAP) Advantage. In fiscal year 2015, TSA used standardized ASAP covert tests conducted by local TSA testers at each airport to measure TSO performance in both the checkpoint and checked baggage environments. Tests focused on checked baggage screening were designed to assess the operational effectiveness of TSOs in identifying and preventing a threat object concealed in a checked bag from being cleared for loading onto a

³⁷This represents the number of first-time tests conducted for specific APR component tests required for the nearly 4,200 TSOs certified to perform checked baggage screening only during calendar year 2015. TSOs certified to perform passenger screening only—roughly 18,000 TSOs in calendar year 2015—or have dual certification to perform both screening functions—approximately 14,400 TSOs in calendar year 2015—take similar, but different APR component tests. For instance, a TSO certified to perform checked baggage screening only must take the APR component test focused on a physical bag search of checked baggage whereas a TSO dual certified to perform both checked baggage and passenger screening would only take the APR component focused on a physical bag search of passengers’ carry-on baggage.

³⁸First-time pass rates for these component tests have been designated as sensitive security information and thus cannot be included in a public report.

passenger aircraft.³⁹ In fiscal year 2015, TSA conducted 1,859 ASAP covert tests on checked baggage screening at 225 airports.⁴⁰

TSA began deploying headquarters-based covert testing teams in fiscal year 2016 to provide a means to validate the results of covert tests conducted by local TSA testers for both checkpoint and checked baggage screening.⁴¹ However, unlike in the checkpoint environment, the contractor did not perform ASAP covert testing on checked baggage screening during fiscal year 2015. When we compared fiscal year 2016 headquarters-based and field-based pass rates for covert testing of checked baggage screening, we found discrepancies that indicate covert tests conducted by local field-based TSA testers on checked baggage may not be reliable in accurately portraying TSO performance. Additionally, TSA officials stated that they cannot be certain these data are reliable. As a result, we do not present ASAP Advantage data in this report.

Checked Baggage Screening Technology and TSA's Checked Baggage Screening System as a Whole

As with checkpoint screening technology discussed above, TSA officials reported that in fiscal year 2015, technology deployed at airports for checked baggage screening was calibrated and tested daily to ensure that it was operating as intended. According to TSA officials, these daily tests help to ensure that its screening technologies are meeting the detection standards they were designed to achieve.⁴² TSA officials

³⁹ASAP tests are designed to automatically trigger checked baggage screening technology to alarm in order to specifically test TSOs' abilities in resolving this alarm. Therefore, ASAP tests are not designed to test the effectiveness of the screening technology itself, but rather to assess the operational effectiveness of TSOs.

⁴⁰In fiscal year 2015, TSA conducted two types of ASAP covert tests—targeted scenarios and standard scenarios. Targeted scenarios are conducted and used at the individual airport level to provide additional TSO training. Standard scenarios are assigned to airports and used to assess results at the national level. In fiscal year 2015, TSA conducted ASAP tests at both SPP and non-SPP airports.

⁴¹According to TSA officials, TSA conducts roughly 8,000 field-based and 4,000 headquarters-based covert tests each year. These operational tests have replaced the ASAP Advantage program.

⁴²TSA also tests the effectiveness of its screening technology through its OOI Red Team Covert Testing. However, as outlined below, these tests are not designed to specifically test the screening technology, but to test the checked baggage screening system as a whole.

reported that any equipment found not to meet required detection standards was immediately taken out of service.⁴³ As described above, OOI also conducted Red Team covert testing on checked baggage screening at airports with EDS machines in fiscal year 2015.⁴⁴ Specific details about TSA's detection standards and the results of OOI's covert tests are omitted because the information is classified.

Explosives Detection Canines

Through its National Explosives Detection Canine Team Program, TSA trains, deploys, and certifies explosives detection canine teams in order to deter and detect the introduction of explosive devices into U.S. transportation systems. Each canine team consists of a handler—generally either a state or local law enforcement officer (LEO) or TSA employee—paired with a canine trained in explosives detection.

⁴³In September 2014, the DHS OIG reported that TSA did not have the capability to independently assess whether deployed EDS machines were operating at the correct detection standards. Instead, they found that TSA relies on daily calibrations by EDS vendor-issued test kits. The DHS OIG recommended that TSA accelerate development and deployment of a test kit to independently validate deployed explosive detection systems equipment performance. TSA concurred and is developing its own EDS test kit to independently validate the effectiveness of the equipment. TSA anticipates deploying the new kits to all airports in 2019.

⁴⁴Results of OOI's Red Team covert tests provide insights about the effectiveness of checkpoint and checked baggage screening, but observations from these airports are not generalizable to all TSA-regulated airports in the United States. OOI officials report that in fiscal year 2015 their Red Team testing included both SPP airports and non-SPP airports.

Figure 6: Transportation Security Administration (TSA) Canine Team Searches an Airport Terminal



Source: TSA. | GAO-17-794

As of September 2015, TSA had 692 canine teams deployed to 88 airports across the United States. These teams were composed of four types of canine teams trained to operate in the airport environment: TSA explosives detection canine (EDC) and Passenger Screening Canine (PSC) teams as well as LEO aviation and multimodal teams. Table 6 shows the number of canine teams by type deployed in the airport environment as of September 2015 and describes their roles and responsibilities.

Table 6: Total Number, Roles, and Responsibilities of Transportation Security Administration (TSA) Canine Teams by Type of Team Deployed in the Aviation Environment as of September 2015

Type of canine team	Number of teams deployed	Description of roles and responsibilities
Law enforcement officer (LEO): aviation	430	Patrol airport terminals, including ticket counters, curbside areas, and secured areas; respond to calls to search unattended items, such as vehicles and baggage; screen air cargo; and serve as general deterrents to would-be terrorists or criminals
LEO: multimodal	26	Patrol and search transportation modes in their geographic area (e.g., aviation, mass transit, and maritime), and screen air cargo
TSA Explosives Detection Canine	92	Patrol and search transportation modes in their geographic area (e.g., aviation, mass transit, or maritime), and screen air cargo

Type of canine team	Number of teams deployed	Description of roles and responsibilities
TSA Passenger Screening Canine	144	Primarily search for explosives odor on passengers in airport terminals
Total	692	

Source: GAO analysis of TSA data. | GAO-17-794

The Effectiveness of Explosives Detection Canines in Fiscal Year 2015

In fiscal year 2015, TSA collected data on the effectiveness of its canine teams in detecting or disrupting threats to aviation security through its annual certification evaluation process and short notice assessments (SNA)—covert tests conducted to assess canine teams’ operational effectiveness in detecting and responding to possible explosives.

Annual Certification Evaluations. TSA’s annual evaluations assess whether canine teams meet the explosives detection certification standards established by the program. Following initial training, new canine teams must demonstrate certain critical skills in order to be certified to work in their home operating environment. After initial certification, all TSA canine teams are evaluated on an annual basis to maintain certification. Canine teams that fail their annual evaluation are decertified and limited to training and operating as a visible deterrent until they successfully complete the annual evaluation and are recertified to conduct screening.⁴⁵

To achieve EDC certification, canine teams must demonstrate their ability to detect hidden explosive training aids across a specified number of areas, a certain percent of the time.⁴⁶ After passing this conventional evaluation, PSC teams undergo further testing in different locations within

⁴⁵In the event a canine team fails an evaluation, an additional assessment is conducted and, based on the findings, an appropriate course of action will be determined by the program. In addition, a corrective action plan is to be created to provide recommendations and guidance to address the canine team’s deficiencies. According to TSA officials, the presence of canine teams in the airport environment provides a deterrent effect to would-be terrorists or criminals.

⁴⁶An explosive training aid is any explosive used to test and train a canine in explosives detection.

the sterile area of an airport.⁴⁷ To achieve PSC certification, canine teams must successfully identify an explosives-carrying target/decoy in a specified number of search areas.

In fiscal year 2015, TSA conducted 673 EDC annual certification evaluations and 116 PSC evaluations. The fiscal year 2015 first-time pass rates for EDC and PSC canine teams has been designated as sensitive security information and thus cannot be included in a public report.

Short Notice Assessments. TSA conducts covert testing of canine teams to measure their effectiveness in detecting and responding to explosives odor during normal operations. These covert tests, known as SNAs, are conducted using one of four scenarios chosen to match a canine team's primary area of operations—an unattended bag, unattended vehicle, cargo screening, and passenger screening. Field Canine Coordinators—TSA officials that administer SNAs—are responsible for debriefing participants after the assessment, determining if corrective actions are necessary, and officially documenting outcomes.

We assessed the reliability of SNA results in fiscal year 2015 and determined that the data were not reliable for the purpose of reporting overall pass rates. Specifically, we found duplicate entries and errors in the data. In addition, we found that fiscal year 2015 data on pass rates may be incomplete since the results of some SNAs may not have been subsequently recorded in TSA's system. Further, TSA's process of manually recording SNA results in fiscal year 2015 lacked procedures to ensure that data entered into TSA's system were accurate and complete.

To address these data limitations, canine program officials stated that a new process was implemented in October 2016 to incorporate SNA results directly into the Canine Website System—a central electronic management database for various canine program data. According to these officials, this new process will better ensure that SNA data are complete, accurate, and reliable for use by program officials and TSA leadership in evaluating the effectiveness of the program.

⁴⁷The sterile area of an airport is the portion in an airport, defined in the airport's security program, that provides passengers access to boarding aircraft and to which the access generally is controlled by TSA through the screening of persons and property. See 49 C.F.R. § 1540.5.

Appendix III: Comments from the Department of Homeland Security

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



**Homeland
Security**

September 5, 2017

Jennifer Grover
Director, Homeland Security and Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management's Response to Draft Report GAO-17-794, "AVIATION SECURITY:
Actions Needed to Systematically Evaluate Cost and Effectiveness Across Security
Countermeasures"

Dear Ms. Grover:

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 of the Transportation Security Administration's (TSA) efforts to improve its analytic methods. Specifically, the report highlighted TSA's Risk and Trade-Space Portfolio Analysis (RTSPA) as "a means for TSA to model its security effectiveness in different scenarios," that it is useful for "informing TSA acquisition and deployment decisions," and that it "could serve as a useful starting place for a more comprehensive system-wide analysis." Furthermore, GAO cited TSA's 2015 decision to deploy an additional 146 Advanced Imaging Technology (AIT) systems as a positive example of decision-making informed by holistic analysis of an entire system of countermeasures.

TSA remains strongly committed to its mission of protecting the Nation's transportation systems to ensure freedom of movement for people and commerce. To help ensure maximum levels of security, TSA continually improves the *effectiveness* of its countermeasures, often in response to evolving adversary tactics. For example, in June 2017, TSA began testing biometric passenger entry for Pre✓[®] lanes. Additionally, TSA improves the efficiency of its countermeasures to reduce burdens on transportation stakeholders, such as the automated screening lanes recently installed in Atlanta, Chicago, New York, and Los Angeles. Countermeasure efficiency is also a function of cost, and while TSA currently reports cost by program area (such as checkpoint or checked-bag screening), DHS agrees that a more granular breakdown by countermeasure (such as for AITs, carry-on x-rays, or explosives trace detectors) would allow for a better understanding of countermeasure impacts, thus leading to better informed procurement decisions.

The Department is also pleased to note GAO's recognition of the significant deterrent component of TSA countermeasures. Since deterrence is a significant component of the security benefit generated by many countermeasures, the Department agrees that this benefit cannot be

ignored. That said, deterrence is fundamentally about the thoughts of our adversaries so developing value estimates of particular countermeasures will never lend itself to a purely scientific process. The Department is committed to bringing a greater level of security to transportation and developing better methods to assess the significant security benefits of deterrence, as appropriate.

TSA has long asserted that perfect security for the Nation's entire transportation system is not practical, and therefore the best strategy is to focus resources on high-risk threats while deterring adversaries by making potential vulnerabilities unclear. For example, the report recognized the benefits of the Federal Air Marshal Service (FAMS) "deployed overseas to counter evolving threats to aviation security." While the report describes deterrence as the FAMS's primary value, other significant benefits exist as well, including measurable contributions to TSA's risk-based security efforts. Principally, FAMS provides dedicated protection for high-risk flights, both as a result of risk-based scheduling methodology that allocates FAM resources in accordance with current risk and threat information, as well as for particular flights identified as higher-risk through the prescreening process. In the event there is concern about a potential attack, FAMS provides resilience and reassurance to the traveling public. These benefits do not fall into the deterrence category, but are no less real, despite also being difficult to quantify.

The draft report contained two recommendations with which the Department concurs. Attached find our detailed response to each of the recommendations.

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

Sincerely,



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

Attachment

**Attachment: DHS Management Response to Recommendations
Contained in GAO-17-794**

GAO recommended that the TSA Administrator:

Recommendation 1: Explore and pursue methods to assess the deterrent effect of TSA's passenger aviation security countermeasures; such an effect should identify FAMS - a countermeasure primarily focused on deterring threats - as a top priority to address.

Response: Concur. Some deterrence contexts, such as illegal immigration or crime in a major city, have thousands or tens of thousands of incidents per unit of time, allowing for the possibility of some kind of "outcome" measurement, such as the reduction in number of incidents (assuming the reduction can be tied to a set of policies and/or countermeasures, which is a separate challenge). In TSA's specific area of Homeland transportation security, incidents are far less frequent. While this is fortunate for the Homeland, it makes measuring the direct outcome problematic and statistically nebulous. Therefore, some proxy measures, such as assessment of the relative deterrence characteristics of TSA's efforts or "output" measures, will be needed. This approach to creating performance measures is consistent with other Office of Management and Budget (OMB) and GAO guidance regarding deterrence measures and very-low-frequency events.

The Risk and Trade-Space Portfolio Analysis (RTSPA) cited in the report is the result of years spent developing TSA risk models, ranging from analyzing the performance of a single countermeasure against an isolated threat (such as an explosive-trace detector's response to a specific underwear-bomb design), to a holistic analysis of a network of countermeasures against a variety of threat scenarios. Unavoidably, some assumptions must be made about potential adversary choices (for example, what is the likelihood of a weapon being concealed on-body, vs. in a carry-on, vs. in a checked-bag?) While informed by the best intelligence and information available, these estimates will always have a subjective element and methods to better evaluate deterrence will be similarly constrained.

The deterrent effect of defensive measures is rarely able to prevent all attacks, but should be thought of in terms of making the adversary shift away from the original attack plan. For example, it is desirable to prospective attackers to: 1) delay their plans (increasing their chance of being caught); 2) switch to less-harmful *targets*; 3) use more difficult *tactics* (such as a less-reliable non-metallic bomb); or 4) expend more *resources* (or some combination). However, it is rare that intelligence provides an explicit window on these effects; and even in those rare circumstances, (as the draft report points out) it is challenging to determine that such an effect was *caused* by a TSA (or other government agency) countermeasure, with even more rare exceptions such as the directions in Inspire 13 to avoid airports utilizing Advanced Imaging Technology. While OMB's and GAO's recommendations to use proxy measures and simulations are helpful, many questions about deterrence accounting remain to be resolved.

As noted in the draft report, TSA's strategic plan seeks more "dynamic resource management" when responding to changing threats and having a greater impact on Agency decisions, but these analytic methods must not result in "analysis paralysis." RTSPA is "refreshed" with new intelligence and effectiveness estimates once per year. TSA believes that expanding RTSPA to include FAMS, or the entire set of TSA countermeasures, would degrade the timeliness and quality of the analysis and require significantly more resources.

TSA will provide GAO a report on its progress in exploring and pursuing methods to assess deterrent effects, in combination with reporting progress to address Recommendation 2, shown below. Estimated Completion Date (ECD): July 31, 2018.

Recommendation 2: As TSA improves the reliability and extent of its information on the effectiveness of aviation security countermeasures, systematically evaluate the potential cost and effectiveness tradeoffs across countermeasures.

Response: Concur. Through the combined efforts of TSA's Office of Requirements and Capabilities Analysis, Office of Acquisitions and Program Management, Office of Chief Performance and Enterprise Risk, as well as others, TSA will continue efforts to improve its robust testing programs and its analysis of the information relating to security effectiveness. TSA's mission is a fundamental balance between mitigating the constant threat of terrorism by deploying countermeasures, while working to ensure the costs and burdens imposed by those countermeasures do not inhibit the transportation sector's vitality. As information about the effectiveness of countermeasures improves, TSA will be able to better account for costs in ways that align with countermeasure effectiveness metrics; thus, informing better cost-benefit decisions for individual countermeasures. TSA continually strives to be more effective and more efficient—for example by developing Pre✓[®] lanes that speed low-risk passengers through screening while simultaneously reducing screening costs. Better cost information will enable continued efficiency improvements.

TSA will provide GAO a report on its progress in evaluating the potential cost and effectiveness tradeoffs, in combination with reporting progress to address Recommendation 1, shown above. ECD: July 31, 2018.

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Jennifer A. Grover, 202-512-7141, groverj@gao.gov

Staff Acknowledgments

In addition to the contact named above, Maria Strudwick (Assistant Director), Chuck Bausell, Claudia Becker, Bryan Bourgault, Bruce Crise, Dominick Dale, Brianna Dieter, Michele Fejfar, Eric Hauswirth, Susan Hsu, James Kernen, and Tom Lombardi made key contributions to this report.

Appendix V: Accessible Data

Data Table

Accessible Data for Figure 2: Examples of Aviation Security Countermeasures Deployed or Expanded, 2001-2017

September 2001 terrorist attacks

November 2001 Aviation and Transportation Security Act

- The Transportation Security Administration (TSA) is created to oversee security in all modes of transportation. Act also requires 100 percent checked baggage screening and expansion of the U.S. Federal Air Marshal Service (FAMS).

June 2002 Checked baggage screening

- TSA begins deployment of explosives detection systems to the more than 400 TSA-regulated airports in the United States in accordance with a mandate in the Aviation and Transportation Security Act to screen 100 percent of checked baggage using explosives detection systems.

April 2003 Federal Flight Deck Officers Program

- The first men and women are sworn in as Federal Flight Deck Officers—i.e., crewmembers authorized to use firearms to defend against acts of criminal violence or air piracy undertaken to gain control of the aircraft — on April 19, 2003, as part of TSA’s Federal Flight Deck Officer Program.

August 2006 FAMS deployed on overseas flights

- TSA increases FAMS deployed overseas to counter evolving threats to aviation security.

September 2006 Enhanced Screening and Bomb Appraisal

- TSA enhances security measures to include more random screening of employees, stronger air cargo security measures,

more rigorous identity verification standards and deploys more security officers trained in behavior detection screening and bomb appraisal.

March 2010 Advanced Imaging Technology

- TSA begins installing hundreds of advanced imaging technology units designed to detect weapons, explosives, and other threats at U.S. airports.

November 2010 Secure Flight

- TSA achieves 100 percent pre-screening for all covered flights to, from, and within the United States using the Secure Flight system.

Cockpit fortification

- TSA and the Federal Aviation Administration work with air carriers to reinforce cockpit doors on commercial aircraft in order to protect from intrusion, small-arms fire and fragmentation devices such as grenades.

Agency Comment Letter

Accessible Text for Appendix III: Comments from the Department of Homeland Security

Page 1

September 5, 2017

Jennifer Grover

Director, Homeland Security and Justice

U.S. Government Accountability Office

441 G Street, NW

Washington, DC 20548

U.S. Department of Homeland Security

Washington, DC 20528

Re: Management's Response to Draft Report GAO-17-794, "AVIATION SECURITY: Actions Needed to Systematically Evaluate Cost and Effectiveness Across Security Countermeasures"

Dear Ms. Grover:

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 of the Transportation Security Administration's (TSA) efforts to improve its analytic methods. Specifically, the report highlighted TSA's Risk and Trade-Space Portfolio Analysis (RTSPA) as "a means for TSA to model its security effectiveness in different scenarios," that it is useful for "informing TSA acquisition and deployment decisions," and that it "could serve as a useful starting place for a more comprehensive system-wide analysis." Furthermore, GAO cited TSA's 2015 decision to deploy an additional 146 Advanced Imaging Technology (AIT) systems as a positive example of decision-making informed by holistic analysis of an entire system of countermeasures.

TSA remains strongly committed to its mission of protecting the Nation's transportation systems to ensure freedom of movement for people and commerce. To help ensure maximum levels of security, TSA continually improves the *effectiveness* of its countermeasures, often in response to evolving adversary tactics. For example, in June 2017, TSA began testing biometric passenger entry for Pre-check lanes. Additionally, TSA improves the efficiency of its countermeasures to reduce burdens on transportation stakeholders, such as the automated screening lanes recently installed in Atlanta, Chicago, New York, and Los Angeles. Countermeasure efficiency is also a function of cost, and while TSA currently reports cost by program area (such as checkpoint or checked-bag screening), DHS agrees that a more granular breakdown by countermeasure (such as for AITs, carry-on x-rays, or explosives trace detectors) would allow for a better understanding of countermeasure impacts, thus leading to better informed procurement decisions.

The Department is also pleased to note GAO's recognition of the significant deterrent component of TSA countermeasures. Since deterrence is a significant component of the security benefit generated by many countermeasures, the Department agrees that this benefit cannot be

Page 2

ignored. That said, deterrence is fundamentally about the thoughts of our adversaries so developing value estimates of particular countermeasures will never lend itself to a purely scientific process. The Department is committed to bringing a greater level of security to transportation and developing better methods to assess the significant security benefits of deterrence, as appropriate.

TSA has long asserted that perfect security for the Nation's entire transportation system is not practical, and therefore the best strategy is to focus resources on high-risk threats while deterring adversaries by making potential vulnerabilities unclear. For example, the report recognized the benefits of the Federal Air Marshal Service (FAMS) "deployed overseas to counter evolving threats to aviation security." While the report describes deterrence as the FAMS's primary value, other significant benefits exist as well, including measurable contributions to TSA's risk-based security efforts. Principally, FAMS provides dedicated protection for high-risk flights, both as a result of risk-based scheduling methodology that allocates FAM resources in accordance with current risk and threat information, as well as for particular flights identified as higher-risk through the prescreening process. In the event there is concern about a potential attack, FAMS provides resilience and reassurance to the traveling public. These benefits do not fall into the deterrence category, but are no less real, despite also being difficult to quantify.

The draft report contained two recommendations with which the Department concurs. Attached find our detailed response to each of the recommendations.

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

Sincerely,

JIM H. CRUMPACKER, CIA, CFE

Director

Departmental GAO-OIG Liaison Office

Attachment

Page 3

Attachment: DHS Management Response to Recommendations
Contained in GAO-17-794

GAO recommended that the TSA Administrator:

Recommendation 1: Explore and pursue methods to assess the deterrent effect of TSA's passenger aviation security countermeasures; such an effect should identify FAMS - a countermeasure primarily focused on deterring threats - as a top priority to address.

Response: Concur. Some deterrence contexts, such as illegal immigration or crime in a major city, have thousands or tens of thousands of incidents per unit of time, allowing for the possibility of some kind of "outcome" measurement, such as the reduction in number of incidents (assuming the reduction can be tied to a set of policies and/or countermeasures, which is a separate challenge). In TSA's specific area of Homeland transportation security, incidents are far less frequent. While this is fortunate for the Homeland, it makes measuring the direct outcome problematic and statistically nebulous. Therefore, some proxy measures, such as assessment of the relative deterrence characteristics of TSA's efforts or "output" measures, will be needed. This approach to creating performance measures is consistent with other Office of Management and Budget (OMB) and GAO guidance regarding deterrence measures and very- low-frequency events.

The Risk and Trade-Space Portfolio Analysis (RTSPA) cited in the report is the result of years spent developing TSA risk models, ranging from analyzing the performance of a single countermeasure against an isolated threat (such as an explosive-trace detector's response to a specific underwear-bomb design), to a holistic analysis of a network of countermeasures against a variety of threat scenarios. Unavoidably, some assumptions must be made about potential adversary choices (for example, what is the likelihood of a weapon being concealed on-body, vs.

in a carry-on, vs. in a checked-bag?) While informed by the best intelligence and information available, these estimates will always have a subjective element and methods to better evaluate deterrence will be similarly constrained.

The deterrent effect of defensive measures is rarely able to prevent all attacks, but should be thought of in terms of making the adversary shift away from the original attack plan. For example, it is desirable to prospective attackers to: 1) delay their plans (increasing their chance of being caught); 2) switch to less-harmful *targets*; 3) use more difficult *tactics* (such as a less-reliable non-metallic bomb); or 4) expend more *resources* (or some combination). However, it is rare that intelligence provides an explicit window on these effects; and even in those rare circumstances, (as the draft report points out) it is challenging to determine that such an effect was caused by a TSA (or other government agency) countermeasure, with even more rare exceptions such as the directions in Inspire 13 to avoid airports utilizing Advanced Imaging Technology. While OMB's and GAO's recommendations to use proxy measures and simulations are helpful, many questions about deterrence accounting remain to be resolved.

Page 4

As noted in the draft report, TSA's strategic plan seeks more "dynamic resource management" when responding to changing threats and having a greater impact on Agency decisions, but these analytic methods must not result in "analysis paralysis." RTSPA is "refreshed" with new intelligence and effectiveness estimates once per year. TSA believes that expanding RTSPA to include FAMS, or the entire set of TSA countermeasures, would degrade the timeliness and quality of the analysis and require significantly more resources.

TSA will provide GAO a report on its progress in exploring and pursuing methods to assess deterrent effects, in combination with reporting progress to address Recommendation 2, shown below. Estimated Completion Date (ECD): July 31, 2018.

Recommendation 2: As TSA improves the reliability and extent of its information on the effectiveness of aviation security countermeasures, systematically evaluate the potential cost and effectiveness tradeoffs across countermeasures.

Response: Concur. Through the combined efforts of TSA's Office of Requirements and Capabilities Analysis, Office of Acquisitions and Program Management, Office of Chief Performance and Enterprise Risk, as well as others, TSA will continue efforts to improve its robust testing programs and its analysis of the information relating to security effectiveness. TSA's mission is a fundamental balance between mitigating the constant threat of terrorism by deploying countermeasures, while working to ensure the costs and burdens imposed by those countermeasures do not inhibit the transportation sector's vitality. As information about the effectiveness of countermeasures improves, TSA will be able to better account for costs in ways that align with countermeasure effectiveness metrics; thus, informing better cost-benefit decisions for individual countermeasures. TSA continually strives to be more effective and more efficient—for example by developing Pre-check lanes that speed low-risk passengers through screening while simultaneously reducing screening costs. Better cost information will enable continued efficiency improvements.

TSA will provide GAO a report on its progress in evaluating the potential cost and effectiveness tradeoffs, in combination with reporting progress to address Recommendation 1, shown above. ECD: July 31, 2018.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

Connect with GAO

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <http://www.gao.gov/fraudnet/fraudnet.htm>
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548