

October 2009

AVIATION SECURITY

DHS and TSA Have Researched, Developed, and Begun Deploying Passenger Checkpoint Screening Technologies, but Continue to Face Challenges



GAO

Accountability * Integrity * Reliability



Highlights of [GAO-10-128](#), a report to congressional requesters

Why GAO Did This Study

Since fiscal year 2002, the Transportation Security Administration (TSA) and the Department of Homeland Security (DHS) have invested over \$795 million in technologies to screen passengers at airport checkpoints. The DHS Science and Technology Directorate (S&T) is responsible, with TSA, for researching and developing technologies, and TSA deploys them. GAO was asked to evaluate the extent to which (1) TSA used a risk-based strategy to prioritize technology investments; (2) DHS researched, developed, and deployed new technologies, and why deployment of the explosives trace portal (ETP) was halted; and (3) DHS coordinated research and development efforts with key stakeholders. To address these objectives, GAO analyzed DHS and TSA plans and documents, conducted site visits to research laboratories and nine airports, and interviewed agency officials, airport operators, and technology vendors.

What GAO Recommends

GAO recommends, among other things, that TSA (1) conduct a risk assessment and develop a cost-benefit analysis and performance measures for passenger screening technologies, and (2) to the extent feasible, ensure that technologies have completed operational tests and evaluations before they are deployed. DHS concurred with the recommendations; however, its implementation plans do not fully address six of the eight recommendations in the report.

[View GAO-10-128](#) or [key components](#). For more information, contact Steve Lord at (202) 512-8777 or lords@gao.gov.

AVIATION SECURITY

DHS and TSA Have Researched, Developed, and Begun Deploying Passenger Checkpoint Screening Technologies, but Continue to Face Challenges

What GAO Found

TSA completed a strategic plan to guide research, development, and deployment of passenger checkpoint screening technologies; however, the plan is not risk-based. According to TSA officials, the strategic plan and its underlying strategy for the Passenger Screening Program were developed using risk information, such as threat information. However, the strategic plan and its underlying strategy do not reflect some of the key risk management principles set forth in DHS's National Infrastructure Protection Plan (NIPP), such as conducting a risk assessment based on the three elements of risk—threat, vulnerability, and consequence—and developing a cost-benefit analysis and performance measures. TSA officials stated that, as of September 2009, a draft risk assessment for all of commercial aviation, the Aviation Domain Risk Assessment, was being reviewed internally. However, completion of this risk assessment has been repeatedly delayed, and TSA could not identify the extent to which it will address all three elements of risk. TSA officials also stated that they expect to develop a cost-benefit analysis and establish performance measures, but officials could not provide timeframes for their completion. Without adhering to all key risk management principles as required in the NIPP, TSA lacks assurance that its investments in screening technologies address the highest priority security needs at airport passenger checkpoints.

Since TSA's creation, 10 passenger screening technologies have been in various phases of research, development, test and evaluation, procurement, and deployment, but TSA has not deployed any of these technologies to airports nationwide. The ETP, the first new technology deployment initiated by TSA, was halted in June 2006 because of performance problems and high installation costs. Deployment has been initiated for four technologies—the ETP in January 2006, and the advanced technology systems, a cast and prosthesis scanner, and a bottled liquids scanner in 2008. TSA's acquisition guidance and leading commercial firms recommend testing the operational effectiveness and suitability of technologies or products prior to deploying them. However, in the case of the ETP, although TSA tested earlier models, the models ultimately chosen were not operationally tested before they were deployed to ensure they demonstrated effective performance in an operational environment. Without operationally testing technologies prior to deployment, TSA does not have reasonable assurance that technologies will perform as intended.

DHS coordinated with stakeholders to research, develop, and deploy checkpoint screening technologies, but coordination challenges remain. Through several mechanisms, DHS is taking steps to strengthen coordination within the department and with airport operators and technology vendors.

Contents

Letter		1
	Results in Brief	6
	Background	9
	TSA Has Taken Actions to Prioritize Investments in Passenger Checkpoint Screening Technologies, but Lacks a Risk-Based Strategy	18
	Ten New Checkpoint Screening Technologies Are in Various Phases of RDT&E, Procurement, and Deployment, but ETP Deployment Has Been Halted	31
	DHS Is Addressing Coordination and Collaboration Challenges with Stakeholders to Research, Develop, and Deploy Checkpoint Screening Technologies	41
	Conclusions	50
	Recommendations for Executive Action	51
	Agency Comments and Our Evaluation	52
Appendix I	Objectives, Scope, and Methodology	57
Appendix II	Comments from the Department of Homeland Security	60
Appendix III	GAO Contact and Staff Acknowledgments	70
Figures		
	Figure 1: TSA Passenger Checkpoint Screening Functions	11
	Figure 2: NIPP Risk Management Framework	16
	Figure 3: Status of Six Checkpoint Screening Technologies that Had Initiated Procurement and/or Deployment as of September 2008	33

Abbreviations

ADRA	Aviation Domain Risk Assessment
AMS	Acquisition Management System
ATSA	Aviation and Transportation Security Act
DHS	Department of Homeland Security
ETP	explosives trace portal
FAA	Federal Aviation Administration
IED	improvised explosive device
IPT	Integrated Product Team
MOU	memorandum of understanding
NIPP	National Infrastructure Protection Plan
PSP	Passenger Screening Program
RD&E	research, development, test and evaluation
RMAT	Risk Management and Analysis Toolset
S&T	Science and Technology Directorate
TSA	Transportation Security Administration
TSL	Transportation Security Laboratory
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.



United States Government Accountability Office
Washington, DC 20548

October 7, 2009

The Honorable James L. Oberstar
Chairman
Committee on Transportation and Infrastructure
House of Representatives

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

The Honorable Jerry F. Costello
Chairman
Subcommittee on Aviation
Committee on Transportation and Infrastructure
House of Representatives

Commercial aircraft have long been a target of terrorism at the hands of hijackers and suicide bombers. The Transportation Security Administration (TSA), the agency with primary responsibility for securing the nation's civil aviation system after the September 11, 2001, terrorist attacks, has identified the need for improved technology to detect explosives and other threat items at airport passenger screening checkpoints to strengthen the nation's defenses against acts of terrorism. From fiscal years 2002 through 2008, over \$795 million has been invested by TSA and the Department of Homeland Security (DHS) for the research, development, test and evaluation (RDT&E), procurement, and deployment of checkpoint screening technologies.

TSA has implemented a multilayered system of security to protect commercial aviation—the most publicly visible layer being the physical screening of passengers and their carry-on items at airport screening checkpoints. TSA's passenger checkpoint screening system—located at all airports regulated by TSA—is comprised of three elements: (1) the personnel, or screeners, responsible for conducting the screening of airline passengers and their carry-on items; (2) the procedures screeners are to follow to conduct screening; and (3) the technology used during the screening process. Collectively, these elements—the people, process and

technology—help to determine the effectiveness and efficiency of passenger checkpoint screening.¹ We previously reported that TSA had made efforts to enhance its passenger checkpoint screening system by strengthening screener training, measuring the performance of screeners and the screening system, and modifying screening procedures to address terrorist threats.²

Within DHS, the Science and Technology Directorate (S&T) and TSA have responsibilities for researching, developing, and testing and evaluating new technologies, including airport checkpoint screening technologies. Specifically, S&T is responsible for the basic and applied research and advanced development of new technologies, while TSA, through its Passenger Screening Program (PSP), identifies the need for new checkpoint screening technologies, provides input to S&T during the research and development of new technologies, which TSA then procures and deploys.³

In 2004, we reviewed DHS's investments in the research and development of technologies to secure the transportation sector, including aviation, and found that DHS needed to strengthen the management of its research and development efforts.⁴ In October 2007, we testified that a key challenge related to securing the homeland involves allocating resources based on

¹TSA screeners are known as Transportation Security Officers and perform a variety of duties related to security and protection of air travelers, airports, and aircraft. TSA further oversees the operations of private sector screeners at airports participating in TSA's Screening Partnership Program.

²GAO, *Aviation Security: Screener Training and Performance Measurement Strengthened, but More Work Remains*, [GAO-05-457](#) (Washington, D.C.: May 2, 2005); and *Aviation Security: Risk, Experience, and Customer Concerns Drive Changes to Airline Passenger Screening Procedures, but Evaluation and Documentation of Proposed Changes Could Be Improved*, [GAO-07-57SU](#) (Washington, D.C.: March 7, 2007).

³In this report, we define basic research as including all scientific efforts and experimentation directed towards increasing knowledge and understanding; applied research as including all efforts directed toward—the solution of specific problems; advanced development as including all efforts directed toward projects that have moved into the development of hardware; and operational testing as verification that new systems are operationally effective, supportable, and suitable.

⁴GAO, *Transportation Security R&D: TSA and DHS Are Researching and Developing Technologies, but Need to Improve R&D Management*, [GAO-04-890](#) (Washington, D.C.: September 30, 2004).

risk.⁵ DHS and TSA leadership have identified that risk-informed considerations will be a cornerstone of departmental and agency policy. In particular, DHS's National Infrastructure Protection Plan (NIPP) stated that TSA should be considering risk management principles when allocating funding for the research and development of security technologies. According to the NIPP, security strategies should be informed by, among other things, a risk assessment that includes threat, vulnerability, and consequence assessments, information such as cost-benefit analyses to prioritize investments, and performance measures to assess the extent to which a strategy reduces or mitigates the risk of terrorist attacks.

In response to your request, this report provides the results of our review of DHS's efforts, through S&T and TSA, to research, develop, and deploy emerging screening technologies for use at airport passenger checkpoints by addressing the following questions: (1) To what extent has TSA developed a risk-informed strategy to prioritize investments in the research and development of passenger checkpoint screening technologies; (2) What new passenger checkpoint screening technologies has DHS researched, developed, tested and evaluated, procured, and deployed since its creation, and why did TSA halt the first technology deployment that it initiated—the explosives trace portal (ETP); and (3) To what extent has DHS coordinated the RDT&E, procurement, and deployment of passenger checkpoint screening technologies internally and with key stakeholders, such as airport operators and technology vendors?

This report is a public version of a restricted report (GAO-09-21SU) that we provided to you earlier this year. In this report in three cases we provide updates regarding the Aviation Domain Risk Assessment (ADRA),

⁵GAO, *Transportation Security: Efforts to Strengthen Aviation and Surface Transportation Security Are Under Way, but Challenges Remain*, [GAO-08-140T](#) (Washington, D.C.: October 16, 2007).

the NIPP, and the number of ETPs in airports.⁶ DHS and TSA deemed some of the information in the restricted report to be sensitive security information, which must be protected from public disclosure. Although this report omits that information, such as specific details associated with the methods and results of testing during the research and development of the ETPs, it addresses the same questions as the restricted report. Also, the overall methodology used for both reports is the same.

To determine the extent to which TSA developed a risk-informed strategy to prioritize investments in the research and development of new checkpoint technologies, we analyzed program documents, including TSA's August 2008 strategic plan for checkpoint technologies, technology project plans, and budget documents. We also compared TSA's strategic plan and DHS's responses regarding their efforts to develop a risk-informed strategy for their research and development investments with DHS's guidance on using risk management principles to prioritize investments and allocate resources.

To determine what new passenger checkpoint screening technologies DHS has researched, developed, tested and evaluated, procured, and deployed, and the reasons why TSA halted the first technology for which it initiated deployment—the ETP, we analyzed TSA's strategic plan, TSA's PSP documentation, technical and operational requirements for new technologies, laboratory test reports, and testing data from operational pilots. Additionally, we interviewed TSA and S&T officials to obtain information on current technologies being researched, developed, and deployed, and conducted site visits to the Transportation Security Laboratory (TSL) and Tyndall Air Force Base to observe testing of new checkpoint technologies. We visited the TSL because that is where S&T tests and evaluates transportation technologies, including checkpoint

⁶ In the April 2009 restricted version of this report, we reported that, as of September 2008, TSA officials could not provide an expected completion date or identify the extent to which the ADRA would address risks to the checkpoint. In this public report on pages 7, 18, and 22, we updated this information and stated that, as of September 2009, TSA officials expected the ADRA to be completed by the end of 2009, but could not identify the extent to which the ADRA would address risks to the checkpoint. Also, in the restricted version of this report, we reported that the NIPP was issued in 2006. In this public report on page 15, we updated this information and stated that DHS issued a new version of the plan in 2009. Furthermore, in the restricted version of this report, we reported that, as of April 2009, TSA had 90 ETPs at airports and 116 ETPs in storage. In this report on page 39, we updated this information and stated that, as of September 2009, 22 ETPs were at airports and no ETPs were in storage.

screening technologies. We visited Tyndall Air Force Base because technologies to detect bottled liquids explosives were being tested there. We also interviewed TSA headquarters officials and senior TSA officials from the airports where TSA had initially deployed or planned to deploy the ETPs, including 29 Federal Security Directors, 1 Deputy Federal Security Director, and 5 Assistant Federal Security Directors for Screening.⁷ We chose these officials because they are the senior TSA officials in charge of security and managing TSA's role in deploying new technologies at the airport. We also visited nine airports and selected these locations based on the technologies that had been deployed or were being tested on site, their geography, size, and proximity to research and development laboratories. Of the nine airports we visited, the ETPs had been deployed or were to be deployed to all of them and other new checkpoint screening technologies were undergoing pilot demonstrations or testing at two of them. We visited four airports on the east coast, three airports on the west coast, and two airports located in the west and southwestern regions of the United States. We selected these locations because they represented small-, medium-, and large-sized airports and different regions in the United States.

To determine the extent to which TSA coordinated and collaborated internally and with key external stakeholders—airport operators and technology vendors—on the RDT&E, procurement, and deployment of checkpoint technologies, we analyzed program documents, including a memorandum of understanding (MOU) between S&T and TSA. Additionally, we interviewed S&T and TSA officials, seven checkpoint technology vendors, and airport operators⁸ and other officials at 40 airports where ETPs had initially been or were to be deployed. Because we selected a nonprobability sample of airports to visit and officials to interview there, we cannot generalize the results of what we learned to airports nationwide. However, the information we gathered from these locations—insights based on observing airport operations and on perspectives of officials who were involved with DHS's efforts to operationally test, evaluate, and deploy checkpoint technologies—could only be obtained through direct observation or from officials stationed at

⁷A Federal Security Director is the ranking TSA authority responsible for the leadership and coordination of TSA security activities at TSA-regulated airports.

⁸TSA defines "airport operator" as any person who operates an airport serving an aircraft operator or foreign air carrier required to have a security program under 49 C.F.R. parts 1544 or 1546. See 49 C.F.R. § 1540.5.

these select sites where technologies were being deployed and tested. We also selected a nonprobability sample of 8 out of the 157 total requirements for the ETP to determine whether some of its key requirements had been tested prior to procuring and deploying the machines.⁹ In addition, we reviewed S&T's and TSA's coordination and collaboration activities and compared them to TSA program guidance and leading practices for collaborating agencies regarding communication, planning, and federal coordination internally and with external stakeholders.¹⁰ Appendix I contains additional information on the objectives, scope, and methodology of our review.

We conducted this performance audit from June 2006 through April 2009, with some updated information as of September 2009 as previously disclosed, 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.

Results in Brief

TSA completed a strategic plan in August 2008, which identified a strategy to invest in the RDT&E, procurement, and deployment of passenger checkpoint screening technologies; however, the plan and its underlying strategy are not risk informed. TSA's strategy does not incorporate some key risk management principles—a risk assessment, cost-benefit analysis, and performance measures—as required by the NIPP. To guide investments in checkpoint screening technologies, TSA officials stated that they consider risks to the checkpoint by analyzing threat information and other factors. However, this approach does not address all three risk elements required by the NIPP, which specifies that risk assessments are to be based on threat, vulnerability, and consequence assessments. Officials stated that they have drafted the Aviation Domain Risk Assessment (ADRA), a risk assessment of the entire aviation sector, including the passenger checkpoint, which is to include an assessment of all three risk elements. TSA officials anticipated finalizing the ADRA in

⁹We selected the eight requirements because they were related to some of the ETP's key functionality requirements, including operational effectiveness, operational suitability, and passenger throughput.

¹⁰GAO, *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, [GAO-06-15](#) (Washington, D.C.: October 21, 2005).

February 2008, but have postponed its completion multiple times. As of September 2009, officials expected completion of the ADRA by the end of calendar year 2009, but could not identify the extent to which the ADRA would address risks to the checkpoint. Therefore, we could not determine when the ADRA will be completed, to what extent it will incorporate all three elements of a risk assessment, and whether it will identify and assess risks to the checkpoint. In addition, TSA officials stated that they have not yet conducted a cost-benefit analysis to set priorities for the PSP, or established performance measures that assess how deployed technologies have reduced or mitigated risk, as required by the NIPP. Officials acknowledged that a cost-benefit analysis and performance measures should be completed; however, they could not provide timeframes for completing them. Without incorporating these DHS risk management principles into the PSP strategy, TSA cannot ensure that it is targeting the highest priority security needs at checkpoints; measure the extent to which deployed technologies reduce the risk of terrorist attacks; or make needed adjustments to its PSP strategy.

S&T and TSA have placed 10 new checkpoint screening technologies in various phases of RDT&E, procurement, and deployment, but halted the deployment of the ETP due to performance problems and high installation costs. TSA has initiated, but not yet completed, deployments of 4 of the 10 technologies; initiated procurements, but not yet deployed, 2 more technologies, including the Whole Body Imager; and has 4 additional technologies, including a shoe scanner, in research and development. In 2006, TSA deployed 101 ETPs to airports, the first deployment of a checkpoint technology initiated by the agency.¹¹ The ETP was deployed even though TSA officials were aware that tests conducted during 2004 and 2005 on earlier ETP models suggested they did not demonstrate reliable performance in an airport environment. Furthermore, the ETP models that were subsequently deployed were not first tested to prove their effective performance in an operational environment, contrary to TSA's acquisition guidance, which recommends such testing. As a result, TSA lacked assurance that the ETP would meet its functional requirements in airports. TSA officials stated that they deployed the machines without resolving these issues to respond quickly to the threat of suicide bombers. After being deployed, the ETPs broke down frequently

¹¹TSA deployed the ETPs from January to June 2006. Since June 2006, TSA removed 11 ETPs from airports due to maintenance issues and placed the ETPs in a warehouse for storage.

and were more expensive to maintain than expected, according to TSA officials. TSA continued to use them at checkpoint lanes even though TSA could not identify whether ETPs were more effective than existing screening procedures. In the future, using validated technologies would enhance TSA's efforts to improve checkpoint security.

DHS S&T and TSA share responsibilities related to the RDT&E, procurement, and deployment of checkpoint screening technologies, and have coordinated and collaborated with each other and key external stakeholders; however, coordination and collaboration challenges remain that DHS is addressing. The Homeland Security Act of 2002 and the Aviation and Transportation Security Act, which established DHS and TSA, respectively, each address the need for coordination and collaboration with stakeholders. S&T and TSA coordination efforts include a 2006 memorandum of understanding for using the TSL, and the establishment of the Capstone Integrated Product Team for Explosives Prevention in 2006 to help DHS, TSA, and the U.S. Secret Service to, among other things, identify priorities for explosives prevention. However, S&T and TSA officials stated that some technology projects were delayed because TSA had not consistently communicated clear requirements to S&T to test technologies, and S&T had not consistently communicated to TSA about projects at the TSL or the time frames to complete them. According to S&T and TSA officials, coordination and collaboration between them has improved since the summer of 2007. TSA has also taken steps to build partnerships with airport operators and technology vendors, such as by hosting conferences with them; however, the agency has not established a systematic process for coordinating with these stakeholders related to passenger checkpoint technologies. For example, 11 of 33 airport operators¹² and 4 of 7 vendors we interviewed told us that TSA had not solicited or shared information with them regarding checkpoint technology needs and priorities. TSA officials acknowledged the need to improve relationships with external stakeholders. According to TSA officials, an Industry Outreach Manager was hired in 2007 and a draft communications plan to provide guidance and a more systematic process to coordinate with these stakeholders is being reviewed, but no completion date could be provided.

¹²We interviewed 46 airport operators, but 13 of them did not express an opinion about whether TSA had shared or solicited information regarding research and development needs and priorities for checkpoint technologies.

To help ensure that DHS's S&T and TSA take a comprehensive, risk-informed approach to the RDT&E, procurement, and deployment of passenger checkpoint screening technologies, and to increase the likelihood of successful procurements and deployments of such technologies, in the restricted version of this report, we recommended that TSA conduct a complete risk assessment, including threat, vulnerability and consequence assessments, that would apply to the PSP; develop cost-benefit analyses to assist in prioritizing investments in new checkpoint technologies; develop quantifiable performance measures to assess the extent to which investments in research and development have mitigated the risks of a terrorist attack; determine if changes need to be made to the PSP strategy as a result of the risk assessment, cost-benefit analyses, and performance measures; to the extent feasible, ensure that operational testing has been successfully completed before deploying checkpoint technologies to airports; and evaluate the benefits and costs of the ETPs currently being used in airports in order to determine whether it is cost effective to continue to use the machines. In written comments on our report, DHS stated that it agreed with our recommendations and identified actions planned or underway to implement them. While DHS is taking steps to address our first and second recommendations related to conducting a risk assessment and cost-benefit analysis, the actions DHS reported TSA had taken or plans to take do not fully address the intent of the remaining recommendations. DHS also provided us with technical comments, which we considered and incorporated in the report where appropriate. In particular, we clarified the wording of a recommendation which originally stated that TSA should develop quantifiable performance measures to assess the extent to which investments in checkpoint screening technologies mitigated the risks of a terrorist attack. We altered the wording to state that performance measures should be developed to assess progress towards security goals.

Background

TSA's airport passenger checkpoint screening system is comprised of three elements: the (1) personnel, or screeners, responsible for operating the checkpoint, including the screening of airline passengers and their carry-on items; (2) standard operating procedures that screeners are to follow to conduct screening; and (3) technology used during the screening process. Collectively, these elements determine the effectiveness and efficiency of passenger checkpoint screening. In strengthening one or more elements of its checkpoint screening system, TSA aims to balance its security goals with the need to efficiently process passengers. We previously reported that TSA had made progress in enhancing its passenger checkpoint screening system by strengthening screener training, measuring the performance of screeners and the screening

system, and modifying screening procedures to address terrorist threats and efficiency concerns.¹³ We made recommendations to DHS designed to strengthen TSA's efforts to train screeners, modify screening standard operating procedures, and measure the performance of the checkpoint screening system. DHS generally agreed with our recommendations and TSA has taken steps to implement them.

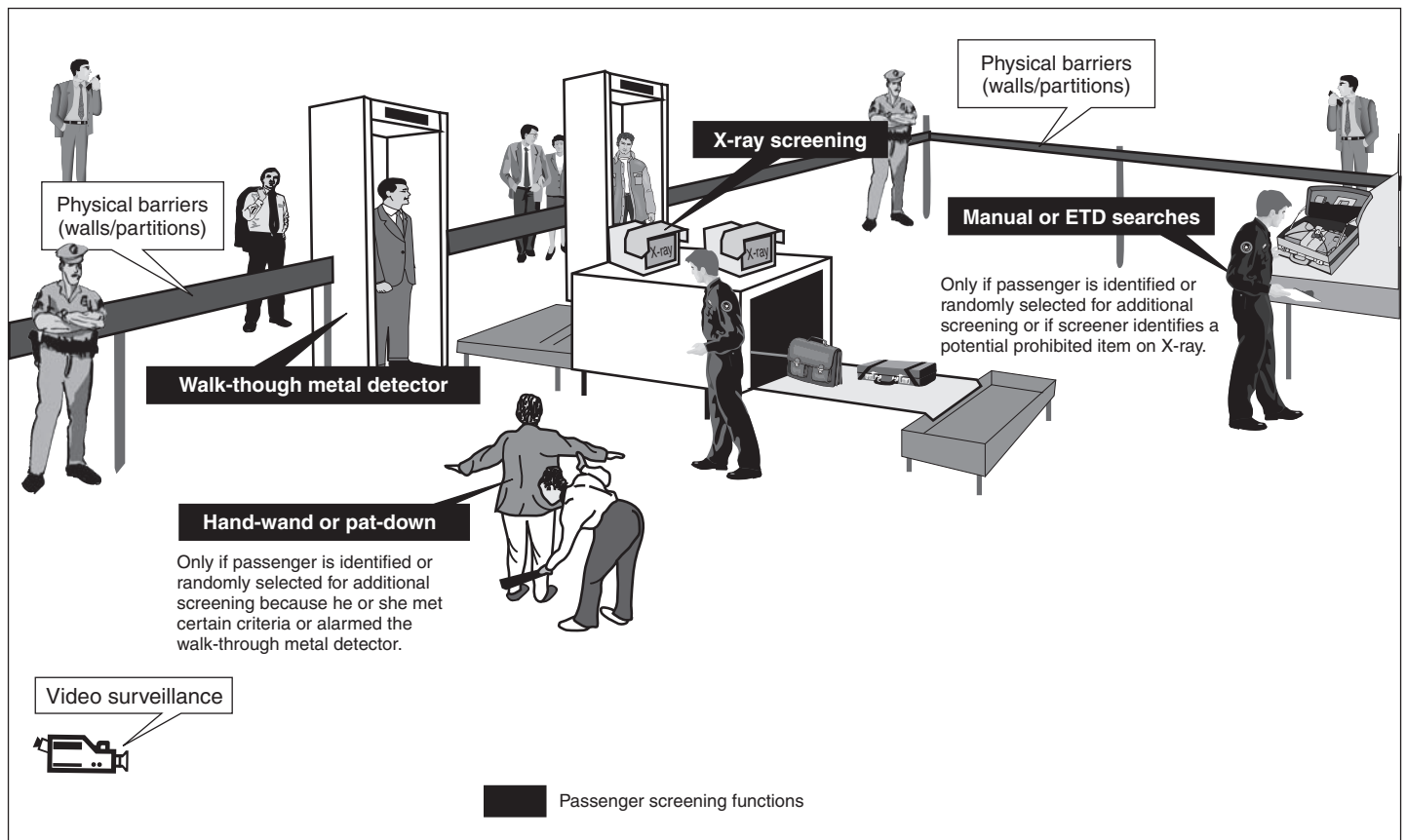
Passenger Checkpoint Screening Process

Passenger screening is a process by which screeners inspect individuals and their property to deter and prevent an act of violence or air piracy, such as the carriage of any unauthorized explosive, incendiary, weapon, or other prohibited item onboard an aircraft or into a sterile area.¹⁴ Screeners inspect individuals for prohibited items at designated screening locations. TSA developed standard operating procedures and the process for screening passengers at airport checkpoints. Figure 1 illustrates the screening functions at a typical passenger checkpoint.

¹³See [GAO-05-457](#) and [GAO-07-57SU](#). We found that TSA had initiated actions designed to enhance screener training; however, screeners sometimes encountered difficulty accessing and completing training due to technological and staffing constraints. We also found that TSA had implemented and strengthened efforts to collect screener and checkpoint performance data through covert testing and a screener recertification program. We further reported that TSA modified standard operating procedures based on risk information, airport staff experiences, and complaints and concerns made by the traveling public, but that TSA could strengthen data collection and analysis to assist in determining whether proposed procedures would achieve their intended purpose.

¹⁴Sterile areas are generally located within the terminal where passengers are provided access to boarding aircraft and access is controlled in accordance with TSA requirements. Access is controlled by screeners—either Transportation Security Officers employed by TSA or nonfederal screeners at airports participating in TSA's Screening Partnership Program—at checkpoints where screening is conducted of individuals and carry-on baggage for weapons, explosives, and other prohibited items. Screeners must deny passage beyond the screening location to any individual or property that has not been screened or inspected in accordance with measures and procedures in place at that checkpoint. If an individual refuses inspection or the inspection of any item, that person or item may not be allowed to enter the sterile area or to board an aircraft.

Figure 1: TSA Passenger Checkpoint Screening Functions



Source: GAO and Nova Development Corporation.

⁸Explosives trace detection (ETD) machines detect small amounts of explosives on or in passenger's carry-on items. ETDs work by detecting vapors and residues of explosives. Human operators collect samples by rubbing bags with swabs, which are chemically analyzed to identify any traces of explosives material.

Primary screening is conducted on all airline passengers prior to entering the sterile area of an airport and involves passengers walking through a metal detector and carry-on items being subjected to X-ray screening. Passengers who alarm the walk-through metal detector or are designated as selectees—that is, passengers selected for additional screening—must

then undergo secondary screening,¹⁵ as well as passengers whose carry-on items have been identified by the X-ray machine as potentially containing a prohibited item. Secondary screening involves additional means for screening passengers, such as by hand-wand, physical pat-down or, at certain airport locations, an ETP, which is used to detect traces of explosives on passengers by using puffs of air to dislodge particles from their body and clothing into an analyzer. Selectees' carry-on items are also physically searched or screened for explosives traces by Explosives Trace Detection (ETD) machines.¹⁶ In addition, DHS S&T and TSA have deployed and are pursuing additional technologies to provide improved imaging or anomaly detection capacities to better identify explosives and other threat objects.

Roles and Responsibilities for the RDT&E, Procurement, and Deployment of Checkpoint Screening Technologies

DHS and TSA share responsibility for the screening of passengers and the research, development, and deployment of passenger checkpoint screening technologies. Enacted in November 2001, the Aviation and Transportation Security Act (ATSA) created TSA and charged it with the responsibility of securing civil aviation, which includes the screening of all passengers and their baggage.¹⁷ ATSA also authorized funding to accelerate the RDT&E of new checkpoint screening technologies. The Homeland Security Act of 2002, enacted in November 2002, established DHS, transferred TSA from the Department of Transportation to DHS and, within DHS, established S&T to have primary responsibility for DHS's RDT&E activities, and for coordinating and integrating all these activities.¹⁸ The Intelligence Reform and Terrorism Prevention Act of 2004

¹⁵A nonselectee passenger who alarms the walk-through metal detector on the first pass is offered a second pass. If the passenger declines the second pass through, the passenger must proceed to additional screening. If the nonselectee passenger accepts the second pass and the machine does not alarm, the passenger may generally proceed without further screening.

¹⁶Passengers are also screened by Behavior Detection Officers under the Screening of Passengers by Observation Techniques (SPOT) program and by Travel Document Checkers. SPOT is an additional layer of security using behavior observations and analysis techniques to identify potentially high-risk individuals based on deviations from environmental baselines. Behavior Detection Officers are tasked with detecting individuals exhibiting behaviors that indicate they may be a threat to aviation and/or transportation security. Travel Document Checkers are specially trained screeners who are positioned in front of the checkpoint to check passengers' boarding passes and identification in order to determine the authenticity of these documents.

¹⁷See Pub. L. No. 107-71, 115 Stat. 597 (2001).

¹⁸See Pub. L. No. 107-296, § 302, 116 Stat. 2135, 2163-64 (2002).

(Intelligence Reform Act), enacted in December 2004, directed the Secretary of Homeland Security to give high priority to developing, testing, improving, and deploying checkpoint screening equipment that detects nonmetallic, chemical, biological, and radiological weapons and explosives, in all forms, on individuals and in their personal property.¹⁹

Until fiscal year 2006, TSA had primary responsibility for investing in the research and development of new checkpoint screening technologies, and was responsible for developmental and operational test and evaluation of new technologies.²⁰ However, during fiscal year 2006, research and development functions within DHS were consolidated, for the most part, within S&T.²¹ After this consolidation, S&T assumed primary responsibility for funding the research, development, and developmental test and evaluation of airport checkpoint screening technologies. S&T also assumed responsibility from TSA for the Transportation Security Laboratory (TSL) which, among other things, tests and evaluates technologies under development. TSA, through the PSP that was transferred from the Federal Aviation Administration (FAA) to TSA, continues to be responsible for identifying the requirements for new checkpoint technologies; operationally testing and evaluating technologies in airports; and procuring, deploying, and maintaining technologies. This transfer of responsibility from TSA to S&T did not limit TSA's authority to acquire commercially available technologies for use at the checkpoint.

DHS and TSA's Processes for the RDT&E, Procurement, and Deployment of Checkpoint Screening Technologies

S&T and TSA's RDT&E, procurement, and deployment efforts are made up of seven components: basic research, applied research, advanced development, operational testing, procurement, operational integration, and deployment. S&T is responsible for conducting basic and applied research, and advanced development, including developmental test and evaluation. TSA is responsible for conducting operational test and evaluation, operational integration, procurement and deployment of new

¹⁹See Pub. L. No. 108-458, § 4013(a), 118 Stat. 3638, 3719-20 (2004) (codified at 49 U.S.C. § 44925(a)).

²⁰Developmental testing is conducted to assist in the development and maturation of a system or subsystem to verify the status of technical progress and certify readiness to enter initial operational testing. Operational testing verifies that new systems are operationally effective, supportable, and suitable before deployment.

²¹DHS undertook to coordinate and integrate most of its research, development, demonstration, testing, and evaluation activities in accordance with section 302(12) of the Homeland Security Act.

technologies, including checkpoint screening technologies. These seven components are described below.

- *Basic research* includes scientific efforts and experimentation directed toward increasing knowledge and understanding in the fields of physical, engineering, environmental, social, and life sciences related to long-term national needs.
- *Applied research* includes efforts directed toward solving specific problems with a view toward developing and evaluating the feasibility of proposed solutions.
- *Advanced development* includes efforts directed toward projects that have moved into the development of hardware and software for field experiments and tests, such as acceptance testing.²²
- *Operational test and evaluation* verifies that new systems are operationally effective, supportable, and suitable before deployment.
- *Operational integration* is the process employed to enable successful transition of viable technologies and systems to the field environment.
- *Procurement* includes the efforts to obtain a product or service.²³
- *Deployment* is a series of actions following the determination that the product meets its requirements and is accepted by the program manager and integrated product team; designated locations are configured for product integration into the screening operating system and the installed product passes site acceptance tests; and logistics support is in place and all users are trained to use the product.

RDT&E, Procurement, and Deployment Funding for Checkpoint Screening Technologies

Over \$795 million has been invested by DHS and TSA during fiscal years 2002 through 2008 for the RDT&E, procurement, and deployment of checkpoint screening technologies. During this time, over \$91 million was invested in the RDT&E of checkpoint technologies and about \$704 million was invested in the procurement and deployment of these technologies. From fiscal years 2002 through 2005, TSA was responsible for the RDT&E of checkpoint technologies; however, TSA officials could not identify the

²²Acceptance testing consists of testing conducted to determine whether a system or, in this case, technology satisfies its acceptance criteria, such as specification requirements, and to enable the customer to determine whether to accept the system or technology.

²³According to TSA officials, depending on the requirements of the sought-after technology and how it will be used, S&T and TSA first try to identify commercial-off-the-shelf (COTS) equipment that meets identified requirements without having to modify it. If COTS equipment is identified but must be modified to meet TSA's needs, it would only be used if it could be modified within a reasonable cost and time frame. If COTS equipment cannot be identified or cannot be modified to meet TSA's requirements within a reasonable cost or time frame, S&T would try to develop a new technology for TSA.

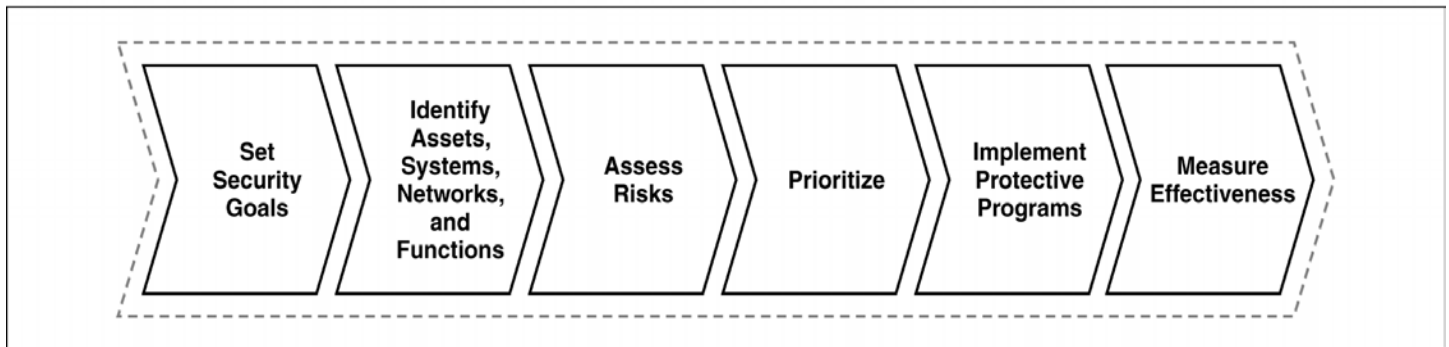
amount of funding the agency invested for these purposes during those years. After fiscal year 2005, TSA invested \$14.5 million for test and evaluation of checkpoint technologies, but did not fund the research and development of these technologies because responsibility in general for research and development funding was transferred from TSA to S&T beginning in fiscal year 2006. Therefore, during fiscal years 2006 through 2008, S&T invested \$77.0 million in the RDT&E of checkpoint screening technologies. All of the approximately \$704 million for the procurement and deployment of checkpoint screening technologies from fiscal years 2002 through 2008 was invested by TSA because the agency has been responsible for procurement and deployment of these technologies since it was created.

Applying a Risk Management Approach to Checkpoint Technology Investments

Risk management is a tool that policy makers can use to help ensure that strategies to develop protective programs and allocate resources target the highest priority security needs. This information helps officials determine which security programs are most important to develop and fund, given that it is not possible to protect the country against all threats because of limited resources. Law and related policy, including the Intelligence Reform Act, the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act), and Homeland Security Presidential Directive 7, provide that federal agencies with homeland security responsibilities are to apply risk-informed principles to prioritize security needs and allocate resources. Consistent with these provisions, DHS issued the National Strategy for Transportation Security in 2005 that, among other things, describes the policies that DHS is to apply when managing risks to the security of the U.S. transportation system. Further, in June 2006, DHS issued the NIPP, which provides a risk management framework to guide strategies to develop homeland security programs and allocate resources to them.²⁴ According to the NIPP, its risk management framework consists of six phases that help to identify and assess risks and prioritize investments in programs, as illustrated in figure 2. The NIPP designated TSA as the primary federal agency responsible for coordinating critical infrastructure protection efforts within the transportation sector.

²⁴DHS, *National Infrastructure Protection Plan* (Washington, D.C.: June 2006). In 2009, DHS issued an updated plan that replaced the one issued in 2006.

Figure 2: NIPP Risk Management Framework



Source: DHS.

A risk-informed strategy to develop and invest in critical infrastructure protection, according to the NIPP, begins with setting security goals. Setting security goals involves defining specific outcomes, conditions, end points, or performance targets that collectively constitute an effective protective posture. Once security goals are established, decisionmakers are to identify what assets or systems to protect and identify and assess the greatest risks to them, that is, the type of terrorist attack that is most likely to occur and that would result in the most severe consequences. Risk of a terrorist attack, according to the NIPP, is to be assessed by analyzing consequences of an attack; the threat—that is, the likelihood of an attack; and the extent to which an asset or a system, in this case the transportation system, is vulnerable to this type of attack.²⁵ The potential consequences of any incident, including terrorist attacks and natural or manmade disasters, is the first factor to be considered in a risk assessment. In the context of the NIPP, consequence is measured as the range of loss or damage that can be expected in the event a terrorist attack succeeds. A consequence assessment looks at the expected worst case or reasonable worst case impact of a successful attack. A threat assessment is the identification and evaluation of adverse events that can harm or damage an asset and takes into account certain factors, such as whether the intent and capability to carry out the attack exist. A vulnerability assessment identifies weaknesses or characteristics of an asset or system, such as its design and location, which make it susceptible to a terrorist

²⁵DHS has adopted an all-hazards mission, which includes both natural disasters and terrorism. The department uses the NIPP to assess risk for both; however, in the context of this report, we are focusing on terrorism. The NIPP provides that for some critical infrastructure sectors, assessing system risk is more appropriate.

attack and that may be exploited. This analysis should also take into consideration factors such as protective measures that are in place which may reduce the risk of an attack and the system's resiliency, that is, ability to recover from an attack.

Once the three components of risk—threat, vulnerability, and consequence—have been assessed for a given asset or system, they are used to provide an estimate of the expected loss considering the likelihood of an attack or other incident. According to the NIPP, calculating a numerical risk score using comparable, credible methodologies provides a systematic and comparable estimate of risk that can help inform national and sector-level risk management decisions. To be considered credible, the NIPP states that a methodology must have a sound basis; be complete; be based on assumptions and produce results that are defensible; and specifically address the three variables of the risk calculus: threat, vulnerability, and consequence. The methodology should also be comparable with other methodologies to support a comparative sector or national risk assessment. To be comparable, a methodology must be documented, transparent, reproducible, accurate, and provide clear and sufficient documentation of the analysis process and the products that result from its use.

The next steps in the DHS risk management framework involve establishing priorities for program development based on risk assessments; implementing these protective programs; and measuring their effectiveness by developing and using performance measures. Identifying and assessing risks helps decisionmakers to identify those assets or systems that are exposed to the greatest risk of attack and, based on this information, prioritize the development and funding of protective programs that provide the greatest mitigation of risk given available resources. The NIPP notes that because resources are limited, risk analysis must be completed before sound priorities can be established. To determine which protective measures provide the greatest mitigation of risk for the resources that are available, the NIPP directs policy makers to evaluate how different options reduce or mitigate threat, vulnerability, or consequence of a terrorist attack. To do so, the NIPP states that cost estimates are combined with risk-mitigation estimates in a cost-benefit analysis to choose between the different options. The last step in the NIPP, measuring the effectiveness of security programs by developing and using performance measures, provides feedback to DHS on its efforts to attain its security goals. Performance metrics are to be developed and used to affirm that specific goals and objectives are being met or to articulate gaps in the national effort or supporting sector efforts. Performance measures

enable the identification of corrective actions and provide decisionmakers with a feedback mechanism to help them make appropriate adjustments in their strategies for protecting critical infrastructure.

TSA Has Taken Actions to Prioritize Investments in Passenger Checkpoint Screening Technologies, but Lacks a Risk-Based Strategy

While TSA completed a strategic plan for the PSP in August 2008 that identifies a strategy for researching, developing, and deploying checkpoint screening technologies, the plan and the strategy were not developed based upon all of the key risk management principles outlined in DHS's NIPP. For instance, TSA has not conducted a complete risk assessment for the PSP, conducted a cost-benefit analysis to prioritize investments, or developed performance measures to assess the extent to which the risk of attack has been reduced or mitigated by investments in technologies. While the agency is currently reviewing a draft of the Aviation Domain Risk Assessment (ADRA), as of September 2009, the ADRA had not been finalized. Officials expect it to be finalized by the end of calendar year 2009. TSA officials could not provide an expected completion date. Therefore, we could not determine when TSA will complete it or to what extent it will be consistent with DHS's risk management framework. TSA officials acknowledged the importance of a cost-benefit analysis and performance measures to guide technology investments, and stated that they intend to develop them, but could not identify when they would be completed. Until TSA completes these activities, the agency lacks assurances that the PSP strategy addresses the highest priority needs and mitigates the risk of an attack. Further, TSA lacks information to adjust its strategy, if needed.

TSA Completed a Strategic Plan for the PSP that Identifies Goals and Objectives

TSA completed a strategic plan in August 2008 that identifies a strategy and establishes goals and objectives for the PSP, and submitted the plan to congressional committees in September 2008.²⁶ However, TSA officials stated that the NIPP was not used as guidance in developing the plan. Instead, the officials stated that the specific requirements for a strategic plan, as outlined in the Intelligence Reform Act and 9/11 Commission Act, were used as guidance to construct the plan. The strategic plan identifies three broad trends that have been observed in the types of threats that TSA faces. First, interest in catastrophic destruction of aircraft and

²⁶Passenger Checkpoint Screening Program Strategic Plan, Aviation Security, Report to Congress in Response to Conference Report 109-699 to the Fiscal Year 2007 Department of Homeland Security Appropriations Bill, August 2008.

facilities has increased, in contrast to hijacking and hostage-taking that characterized the majority of earlier attacks. Second, the range of encountered weapons has expanded, many not previously recognized as threats, nor detected by the technologies that were deployed. Third, terrorists have attacked “soft” airport targets, including airport lobbies, in other countries. To address these challenges, TSA’s strategic plan identifies that the agency’s strategy is to utilize intelligence; partner with law enforcement, industry partners, and the public; and implement security measures that are flexible, widely deployable, mobile, and layered to address the nation’s complex open transportation network. According to the plan, TSA is in the process of implementing and evaluating a fundamental shift in strategy for the security checkpoint that encompasses the critical elements of people, process, and technology. In addition, the plan states that implementing a new security approach called Checkpoint Evolution,²⁷ which started in the spring 2008, will bring the most significant changes that have occurred in passenger screening since the airport security checkpoint was first established in the 1970s.

TSA’s strategic plan identifies that the key component of TSA’s strategy related to security checkpoints is to improve security effectiveness and resource utilization at the checkpoints. Also, the PSP manager stated that a goal of the PSP strategy is to achieve full operating capability by the dates discussed for each checkpoint screening technology listed in the strategic plan. To meet these goals, the PSP strategic plan identifies three strategic objectives: (1) improve explosive detection capability, (2) improve the behavior detection capability of Transportation Security Officers (TSO), and (3) extend the layers of security throughout the passenger journey. The first objective, improving explosive detection capability, involves combining new technology with procedures that emphasize an element of unpredictability to improve explosive detection capability and prevent would-be attackers from knowing the TSA security process. The second objective, improving the behavior detection capability of TSOs, involves shaping the checkpoint environment to better support and enhance behavior detection capabilities by enabling TSOs to engage a larger number of passengers more frequently throughout the checkpoint queue using informal interviews and SPOT; improving the observation conditions for TSOs trained in SPOT by enhancing the

²⁷According to TSA, Checkpoint Evolution is a new security approach that involves many different elements to secure the checkpoint including continuously adapting security procedures to improve passenger security.

contrast between passengers exhibiting signs of travel stress and those intending to do harm to other passengers, aircraft, or the airport; and providing communications tools for enhanced coordination between TSOs trained in SPOT. The third objective, extending the layers of security throughout the passenger journey, involves enabling additional layers of non-intrusive security beyond the checkpoint and into public spaces; increasing the interaction between TSOs and passengers to provide more opportunities to identify irregular behaviors far ahead of the potential threat reaching the checkpoint; and partnering with airlines, airports, and the private sector to reduce vulnerabilities in soft target areas.

TSA had been directed on multiple occasions to provide strategic plans for explosives detection checkpoint technologies to congressional committees. The Intelligence Reform Act mandated that TSA provide a strategic plan that included, at a minimum, a description of the current efforts to detect explosives on individuals and in their personal property; operational applications of explosive detection equipment at airport checkpoints; quantities of equipment needed to implement the plan and a deployment schedule; funding needed to implement the plan; measures taken and anticipated to be taken to provide explosives detection screening for all passengers identified for additional screening; and recommended legislative actions, if any.²⁸ The Intelligence Reform Act mandated that such a strategic plan be submitted to congressional committees during the second quarter of fiscal year 2005. According to TSA officials, a strategic plan was developed and delivered to congressional committees on August 9, 2005, in satisfaction of the statutory mandate. However, the 9/11 Commission Act, enacted August 3, 2007, reiterated a requirement for a strategic plan that TSA was mandated to submit in accordance with the Intelligence Reform Act. Specifically, the 9/11 Commission Act required that the Secretary of Homeland Security issue a strategic plan addressing its checkpoint technology program not later than 30 days after enactment of the 9/11 Commission Act (that is, by September 3, 2007) and required implementation of the plan to begin within 1 year of the act's enactment.²⁹ In response to the 9/11 Commission Act, TSA provided to Congress the Aviation Security Report: Development

²⁸ See 49 U.S.C. § 44925(b).

²⁹ See Pub. L. No. 110-53, § 1607, 121 Stat. at 483.

of a Passenger Checkpoint Strategic Plan, September 2007.³⁰ Finally, Division E of the Consolidated Appropriations Act, 2008, enacted on December 26, 2007, required that the Secretary of Homeland Security submit a strategic plan for checkpoint technologies no later than 60 days after enactment of the Act (that is, by February 25, 2008), and further restricted the use of \$10,000,000 appropriated to TSA for Transportation Security Support until the Secretary submitted the plan to the Committees on Appropriations of the Senate and House of Representatives.³¹ As a result of the mandate for a strategic plan and the funding restriction in the 2008 Consolidated Appropriations Act, TSA officials told us that they interpreted this legislative language to mean that congressional committees considered TSA's aviation security report in September 2007 to be incomplete and insufficient. After approximately 12 months had elapsed since a strategic plan had been mandated in the 9/11 Commission Act, in August 2008 TSA completed its revised strategic plan and delivered it to the committees in September 2008, which TSA officials stated meets the mandate for a strategic plan in the 9/11 Commission Act, as well as the mandate for a strategic plan in the appropriations act.

As previously discussed, the Intelligence Reform Act included requirements for a deployment schedule, and descriptions of the quantities of equipment and funding needed to implement the plan.³² However, our analysis of TSA's August 2008 strategic plan indicates that the strategic plan could include more complete information about these requirements. For example, although TSA provided some deployment information for each emerging checkpoint technology listed in the strategic plan—such as the total quantity to be deployed, expected full operating capability date, and types or categories of airports where the equipment is to be deployed—it does not include a year-by-year schedule showing the number of units for each emerging technology that is expected to be deployed to each specific airport. Regarding information on the funding needed to implement the strategic plan, it includes a funding profile for each fiscal year from 2007 through 2009. However, a number of the

³⁰ The strategic plan mandated by the Intelligence Reform and 9/11 Commission Acts was to be submitted to the Senate Commerce, Science, and Transportation Committee and the House of Representatives Transportation and Infrastructure Committee.

³¹ See Pub. L. No. 110-161, Div. E, 121 Stat. at 1844, 2053 (2007) (referencing H.R. Conf. Rep. No. 109-699, at 138 (Sept. 28, 2006), which had initially directed TSA to develop and submit this plan to the committees).

³² See 49 U.S.C. § 44925(b)(2).

emerging technologies are not expected to reach full operating capability until fiscal year 2014. TSA officials stated that they have derived notional (that is, unofficial) quantities to be deployed on an annual basis for each technology through its respective full operating capability date, but the officials stated that the funding profile in the strategic plan does not reflect the funding needed for these future quantities because the funding that will be appropriated for them after fiscal year 2009 is unknown. According to the officials, to implement the strategic plan in the years beyond fiscal year 2009, the agency intends to use a year-by-year approach whereby the quantities to be deployed in a particular year, and the funding needed for that year, would not be officially identified prior to the budget request for that year.

TSA officials stated that they used risk to inform the August 2008 strategic plan and the PSP strategy identified in it. Although TSA may have considered that risk to some degree, our analysis does not confirm that these efforts meet the risk-based framework outlined in the NIPP. Specifically, TSA has not conducted a risk assessment or cost-benefit analyses, or established quantifiable performance measures. As a result, TSA does not have assurance that its efforts are focused on the highest priority security needs, as discussed below.

TSA Has Not Conducted a Risk Assessment to Inform Its PSP Strategy, but Is Finalizing an Assessment and Developing Information that May Help Guide PSP Efforts

TSA has not conducted a risk assessment that includes an assessment of threat, vulnerability, and consequence, which would address passenger checkpoint screening; consequently, the PSP strategy has not been informed by such a risk assessment as required by the NIPP. Agency officials stated that they prepared and are currently reviewing a draft of a risk assessment of the aviation domain, known as the ADRA, which is expected to address checkpoint security and officials expect it to be finalized by the end of calendar year 2009; however, its completion has been delayed multiple times since February 2008. Therefore, it is not clear when this assessment will be completed. The ADRA, when completed, is to provide a scenario-based risk assessment for the aviation system that may augment the information TSA uses to prioritize investments in security measures, including the PSP. However, officials could not provide details regarding the extent to which the ADRA would assess threat, vulnerability, and consequence related to the passenger checkpoint. In 2004, we recommended that the Secretary of Homeland Security and the Assistant Secretary for TSA complete risk assessments—including a

consideration of threat, vulnerability, and consequence—for all modes of transportation, and use the results of these assessments to help select and prioritize research and development projects.³³ TSA and DHS concurred with the recommendation, but have not completed these risk assessments. Because TSA has not issued the ADRA or provided details regarding what it will entail, and because it is uncertain when the ADRA will be completed, it is not clear whether the ADRA will provide the risk information needed to support the PSP and TSA’s checkpoint technology strategy. In the meantime, TSA has continued to invest in checkpoint technologies without the benefit of the risk assessment information outlined in the NIPP. Consequently, TSA increases the possibility that its investments will not address the highest priority security needs.

Although TSA has not completed a risk assessment to guide its PSP, officials stated that they identify and assess risks associated with the passenger screening checkpoint by relying on threat information, vulnerability information from Threat Image Projection (TIP) scores, limitations of screening equipment identified during laboratory testing, covert tests, and expert judgment to guide its investment strategy in the PSP.³⁴ Specifically, TSA’s Office of Intelligence produces civil aviation threat assessments on an annual basis, among other intelligence products. These assessments provide information on individuals who could carry out attacks, tactics they might use, and potential targets. TSA’s most recent aviation threat assessment, dated December 2008, identifies that terrorists worldwide continue to view civil aviation as a viable target for attack and as a weapon that can be used to inflict mass casualties and economic damage. It also concluded that improvised explosive devices (IED) and hijackings pose the most dangerous terrorist threat to commercial airliners in the United States. The assessment identifies that these devices may be concealed on persons, disguised as liquids, or hidden within everyday, familiar objects such as footwear, clothing, toys, and

³³GAO-04-890.

³⁴The Threat Image Projection (TIP) system places images of threat objects on the X-ray screen during actual operations and records whether screeners identify the threat object. TIP is designed to test screeners’ detection capabilities by projecting threat images, including guns and explosives, into bags as they are screened. Screeners are responsible for positively identifying the threat image and calling for the bag to be searched. Once prompted, TIP identifies to the screener whether the threat is real and then records the screener’s performance in a database that could be analyzed for performance trends. Low performance makes the screening process vulnerable to terrorist attempts to smuggle such materials onto aircraft.

electronics. The threat assessment further identifies that terrorists have various techniques for concealing explosives on their persons. In addition to the annual civil aviation threat assessment, the Office of Intelligence prepares for TSA's senior leadership team and other officials a (1) daily intelligence briefing, (2) tactical intelligence report that is produced one to four times per week, (3) weekly field intelligence summary, (4) weekly suspicious incident report, and, when necessary, (5) special events update, for example, during major political events. However, according to the NIPP, relying on threat information is not sufficient to identify and assess risks. Rather, threat information, which indicates whether a terrorist is capable of carrying out a particular attack and intends to do so, is to be analyzed along side information on vulnerabilities—weakness in a system that would allow such an attack to occur—and on the consequences of the attack, that is, the results of a specific type of terrorist attack, according to the NIPP.

TSA officials stated that, to guide the PSP, they also rely on programs in place that are designed to assess vulnerabilities at airport checkpoints. To identify vulnerabilities at airport checkpoints, TSA officials stated that TSA analyzes TIP scores, known limitations of screening equipment based on laboratory testing, and information from its covert testing program. TSA conducts national and local covert tests, whereby individuals attempt to enter the secure area of an airport through the passenger checkpoint with a prohibited item in their carry-on bags or hidden on their person. Officials stated they use these sources of information to identify needed changes to standard screening procedures, new technology requirements, and deployment strategies for the PSP. When a checkpoint vulnerability is identified, officials stated that TSA's Office of Security Technology engages other TSA stakeholders through the PSP's Integrated Project Team process³⁵ to identify and develop necessary technology requirements which may lead to new technology initiatives. Officials credited this process with helping TSA identify needed changes to standard screening procedures and deployment strategies for new technologies. For example, according to a TSA official, a technology was developed as a result of tests conducted by GAO that found that prohibited items and components of an

³⁵ TSA manages the PSP, in part, through an Integrated Product Team (IPT), which is led by the PSP, but draws its members from across TSA, including the Office of Security Operations and the Office of Acquisitions.

IED might be more readily identified if TSA were to develop new screening technologies to screen these items.³⁶

Although TSA has obtained information on vulnerabilities at the screening checkpoint, the agency has not assessed vulnerabilities (that is, weaknesses in the system that terrorists could exploit in order to carry out an attack) related to passenger screening technologies that are currently deployed. The NIPP requires a risk assessment to include assessments of threat, vulnerability, and consequence. TSA has not assessed whether there are tactics that terrorists could use, such as the placement of explosives or weapons on specific places on their bodies, to increase the likelihood that the screening equipment would fail to detect the hidden weapons or explosives. Although TIP scores measure how effectively screeners identify prohibited items, they do not indicate whether screening technologies currently deployed may be vulnerable to tactics used by terrorists to disguise prohibited items, such as explosives or weapons, thereby defeating the screening technologies and evading detection. Similarly, TSA's covert testing programs do not systematically test passenger and baggage screening technologies nationwide to ensure that they identify the threat objects and materials the technologies are designed to detect, nor do the covert testing programs identify vulnerabilities related to these technologies. We reported in August 2008 that, while TSA's local covert testing program attempts to identify test failures that may be caused by screening equipment not working properly or caused by screeners and the screening procedures they follow, the agency's national testing program does not attribute a specific cause of the test failure.³⁷ We recommended, among other things, that TSA require the documentation of specific causes of all national covert testing failures, including documenting failures related to equipment, in the covert testing database to help TSA better identify areas for improvement. TSA concurred with this recommendation and stated that the agency will expand the covert testing database to document test failures related to screening equipment. Moreover, TSA officials stated that it is difficult to attribute a test failure to equipment, because there is a possibility that the threat item used for the test was not designed properly and, therefore,

³⁶The work related to the tests conducted by GAO contains classified material and the results of these tests are not publicly available.

³⁷GAO, *Transportation Security: TSA Has Developed a Risk-Based Covert Testing Program, but Could Better Mitigate Aviation Security Vulnerabilities Identified Through Covert Tests*, [GAO-08-958](#) (Washington, D.C.: August 8, 2008).

should not have set off the equipment's alarm. TSA officials also stated that it is difficult to identify a single cause for a test failure because covert testing failures can be caused by multiple factors. As a result, TSA lacks a method to systematically test and identify vulnerabilities in its passenger and baggage screening equipment in an operational airport setting. Consequently, TSA officials do not have complete information to identify the extent to which existing screening technologies mitigate vulnerabilities at the passenger checkpoints, so that they can incorporate this information into the agency's security strategy, as required by DHS guidance.

TSA's ADRA, once completed, is to cover the entire aviation domain and include three parts—assessments of over 130 terrorist attack scenarios to determine whether they pose a threat to the aviation system; an assessment of known vulnerabilities or pathways within the aviation system through which these terrorist attacks could be carried out; and an assessment of consequences of these various types of terrorist attacks, such as death, injury, and property loss. TSA officials stated that, through the use of expert panels, the ADRA will evaluate these threat scenarios to assess the likelihood that terrorists might successfully carry out each type of attack on the aviation system, and the likelihood and consequences of these various scenarios will be prioritized to identify the most pressing risks that need to be addressed. In the case of the passenger screening checkpoint, according to officials, TSA will be examining all security measures that a terrorist must breach in order to carry out a specific type of an attack, such as carrying an IED on board an aircraft and detonating it midflight. However, officials could not explain or provide documentation identifying the extent to which the ADRA will provide threat, vulnerability, and consequence assessments in support of the PSP. In addition, the completion date for the ADRA has been delayed multiple times. Because the ADRA has not been finalized and TSA has not described how the ADRA will address the passenger checkpoint, we could not determine the extent to which it will incorporate information on checkpoint

vulnerabilities, including vulnerabilities associated with screening technologies and standard operating procedures.³⁸

In addition to the ADRA, TSA and DHS S&T are developing other information that could inform their identification and assessments of risks to the aviation transportation system. Specifically, TSA and S&T are reviewing the scientific basis of their current detection standards for explosives detection technologies to screen passengers, carry-on items and checked baggage. As part of this work, TSA and S&T are conducting studies to update their understanding of the effects that explosives may have on aircraft, such as the consequences of detonating explosives on board an in-flight aircraft. Senior TSA and DHS S&T officials stated that the two agencies decided to initiate this review because they could not fully identify or validate the scientific support requiring explosives detection technologies to identify increasingly smaller amounts of some explosives over time as required by TSA policy. Officials stated that they used the best available information to originally develop detection standards for explosives detection technologies. However, according to these officials, TSA's understanding of how explosives affect aircraft has largely been based on data obtained from live-fire explosive tests on aircraft hulls at ground level. Officials further stated that due to the expense and complexity of live-fire tests, FAA, TSA, and DHS collectively have conducted only a limited number of tests on retired aircraft, which limited the amount of data available for analysis. As part of this ongoing review, TSA and S&T are simulating the complex dynamics of explosive blast effects on an in-flight aircraft by using a computer model based on advanced software developed by the national laboratories. TSA believes that the computer model will be able to accurately simulate hundreds of explosives tests by simulating the effects that explosives will have when

³⁸The ADRA is part of TSA's efforts to meet the requirements of Homeland Security Presidential Directive 16 (HSPD-16), which requires the DHS Secretary, in coordination with the Secretaries of State, Defense, Commerce, and Transportation, the Attorney General, and the Director of National Intelligence, to prepare a National Strategy for Aviation Security that provides an overarching national strategy to optimize and integrate governmentwide aviation security efforts. The national strategy and its supporting plans are to use a risk-based approach to ensure that national resources are allocated to security efforts with the greatest potential to prevent, detect, defeat, or minimize the consequence of an attack, taking into consideration threat, vulnerabilities, and probable consequences of an attack. The Secretaries of Homeland Security and Transportation are also to lead, in conjunction with the Secretaries of State, Defense, and Energy, and the Attorney General, an interagency effort, in consultation with appropriate industry representatives, to develop and execute a risk-based implementation plan for the continued reduction of vulnerabilities within the Aviation Transportation System.

placed in different locations within various aircraft models. Officials estimated this work will be completed in 3- to 4-month increments through 2008 and 2009. Officials further stated that the prototype version of the model was validated in the late summer of 2008, and that the model is currently being used. TSA and S&T officials stated that they expect the results of this work will provide a much fuller understanding of the explosive detection requirements and the threat posed by various amounts of different explosives, and will use this information to determine whether any modifications to existing detection standards should be made moving forward.

TSA Has Not Completed a Cost-Benefit Analysis to Help Establish Risk-Based Priorities and Guide Its Investment Strategy

TSA has not completed a cost-benefit analysis to prioritize and fund the PSP's priorities for investing in checkpoint technologies, as required by the NIPP's risk management framework. According to the NIPP, policy makers who are designing programs and formulating budgets are to evaluate how different options reduce or mitigate threat, vulnerability, or consequence of a terrorist attack through a cost-benefit analysis that combines cost estimates with risk-mitigation estimates.³⁹ However, in addition to lacking information on risks to the screening checkpoint, TSA has not conducted a cost-benefit analysis of checkpoint technologies being researched and developed, procured, and deployed. Such a cost-benefit analysis is important because it would help decisionmakers determine which protective measures, for instance, investments in technologies or in other security programs, will provide the greatest mitigation of risk for the resources that are available.

One reason that TSA may have difficulty developing a cost-benefit analysis for the PSP is that it has not developed life-cycle cost estimates of each screening technology the PSP is developing, procuring, or deploying. This information is important because it helps decisionmakers determine, given the cost of various technologies, which technology provides the greatest mitigation of risk for the resources that are available. TSA officials prepared a PSP lifecycle cost estimate in September 2005, but this estimate does not include cost estimates for all technologies currently being researched, developed, tested and evaluated, procured and/or deployed, such as the Advanced Technology Systems, a technology to

³⁹ According to the NIPP, investments in protective programs should be prioritized based on a cost benefit analysis that weighs the cost, time, and other characteristics of potential solutions, along with the potential that these various investments in countermeasures will reduce or mitigate threat, vulnerability, or consequence of an attack.

screen carry-on items that TSA is currently procuring. TSA was subsequently instructed by DHS Joint Requirements Council⁴⁰ to complete lifecycle cost estimates for the PSP; in December 2005, the council reviewed the PSP and approved it to proceed to the Investment Review Board for an annual review and potential approval of the PSP's fiscal year 2006 procurement strategy. However, the council expressed concern about several issues that should be resolved prior to the Investment Review Board's review, including the need for complete lifecycle cost estimates for the checkpoint screening technologies that were to be developed and procured. TSA officials acknowledged that completing lifecycle cost estimates are important and stated that they have not prepared a lifecycle cost estimate since the council recommended that such an estimate be developed due to lack of staff. These officials further stated that TSA hired four full-time equivalent staff in fiscal year 2008, and two additional full-time equivalent staff are expected to be hired in the fall of 2008. The officials anticipate that these staff will help prepare lifecycle cost estimates. However, the officials did not provide a timeframe for the completion of the estimates.

Although TSA officials identified the technologies they are procuring and deploying, TSA officials could not provide us with information on their priorities for the research and development of checkpoint screening technologies or the processes they followed to develop these priorities. According to S&T officials, TSA provided priorities for near-term applied research and development projects to the S&T Capstone Integrated Product Team (IPT) for Explosives Prevention.⁴¹ This IPT establishes priorities for research projects to be funded by S&T during the fiscal year. S&T officials stated that they rely on TSA and other members of the IPT to use a risk-based approach to identify and prioritize their agencies' or offices' individual research and development needs prior to submitting them for consideration to the IPT. However, TSA officials stated they did not submit priorities for research and development to S&T. Without cost-benefit or other analysis to compare the cost and effectiveness of various solutions, the agency cannot determine whether investments in the

⁴⁰ The role of the DHS Joint Requirements Council is, among other things, to manage investment portfolios and review projects to identify cross-functional requirements and applications.

⁴¹ In April 2008, S&T dissolved the IPT for explosives detection and replaced it with two separate IPTs, a transportation security IPT, chaired by TSA and a counter-IED IPT, chaired by the Office for Bombing Prevention within the National Protection and Programs Directorate and the United States Secret Service.

research and development of new checkpoint technologies or procedures most appropriately mitigate risks with the most cost-effective use of resources. In addition, without knowing the full cost of the technologies that the PSP is developing, procuring, or deploying, TSA could potentially invest in a technology in which the cost outweighs expected benefits.

TSA Lacks Measures to Evaluate the Extent to Which the PSP Reduces the Risk of Terrorist Attacks

TSA's strategy for the PSP does not have a mechanism—such as performance measures or other evaluation methods—to monitor, assess, or test the extent to which investments in new checkpoint technologies reduce or mitigate the risk of terrorist attacks. The NIPP requires that protective programs be designed to allow measurement, evaluation, and feedback based on risk mitigation so that agencies may re-evaluate risk after programs have been implemented and take corrective action if needed, such as modifying existing programs to counter new risks or implementing alternative programs. The NIPP identifies three types of performance measures—descriptive, process/output, and outcome measures—that can help gauge the effectiveness of protective programs.⁴² Although the NIPP requires that protective programs be designed to allow measurement, evaluation, and feedback based on risk mitigation, TSA has not identified quantifiable measures of progress which would allow the agency to assess the PSP's overall effectiveness. TSA officials stated that they do not have overall performance measures but are currently developing performance goals and measures for the overall program. However, the officials could not provide a time frame for their completion. In September 2004, we recommended that TSA complete strategic plans for its research and development programs which contain measurable

⁴²Descriptive measures are used to understand sector resources and activities, such as the number of facilities in a jurisdiction. Process/output measures are used to measure whether specific activities were performed as planned, tracking the progression of a task, or reporting on the output of a process, such as inventorying assets. Outcome measures track progress towards a strategic goal by beneficial results rather than level of activity. In addition to the NIPP, the Government Performance and Results Act of 1993 provides, among other things, that federal agencies establish program performance measures, including the assessment of relevant outputs and outcomes of each program activity. According to the Office of Management and Budget (OMB), performance goals are target levels of performance expressed as a measurable objective, against which actual achievement can be compared. Performance goals should incorporate measures (indicators used to gauge performance); targets (characteristics that tell how well a program must accomplish the measure), and time frames.

Ten New Checkpoint Screening Technologies Are in Various Phases of RDT&E, Procurement, and Deployment, but ETP Deployment Has Been Halted

objectives.⁴³ Without measures to monitor the degree to which the TSA's investments in the research, development, and deployment of new screening technologies reduce or mitigate terrorist threats, the agency is limited in its ability to assess the effectiveness of the PSP or the extent to which it complements other layers of security at the checkpoint.

Since TSA's creation in 2001, 10 new checkpoint screening technologies, including the ETP, have been in various phases of RDT&E, procurement, and deployment, but TSA halted deployment of the ETP due to performance problems and high installation costs. Of the 10 technologies, TSA has initiated deployments for 4 of them, including the ETP and a Bottled Liquids Scanner, but TSA has not deployed any of the 4 technologies to airports nationwide. TSA also initiated procurements of two technologies, including the Whole Body Imager; however, deployment of these two technologies has not begun yet. Four checkpoint technologies are in research and development, such as a shoe scanning device. In June 2006, 6 to 11 months after TSA began to deploy the ETPs to airports, the agency halted their deployment due to performance problems—the machines broke down more frequently than specified by the functional requirements and the machines were more expensive to install and maintain in airports than expected. Because TSA did not follow its acquisition guidance that recommends technologies be tested and evaluated in an operational setting prior to procurement and deployment, the agency lacked assurance that the ETPs performed as required by the system's requirements. Although TSA officials were aware that tests conducted on earlier ETP models during 2004 and 2005 suggested that they did not operate reliably in an airport environment and that the ETP models that were subsequently deployed to airports had not been tested in an operational environment to prove their effectiveness, TSA deployed the

⁴³In [GAO-04-890](#), we recommended that the Secretary of Homeland Security and the Assistant Secretary for TSA complete strategic plans containing measurable objectives for DHS's and TSA's transportation security research and development programs. DHS stated that it had completed a strategic plan and that TSA was developing a strategic plan that outlined measurable objectives. However, TSA has not yet completed a risk-based plan that outlines measurable objectives. TSA's August 2008 strategic plan for the PSP states that each technology is assessed in the laboratory and in the field using key performance measures, which are reported to senior management, so a decision about whether to acquire the technology can be made. However, these measures apply to the performance of individual, specific technologies against their functional requirements before they are deployed, whereas the NIPP guidance refers to performance measures that assess the effectiveness of a program as a whole to mitigate risk and improve security.

ETPs to airports beginning in July 2005 for the Smiths Detection ETP and beginning in January 2006 for the General Electric ETP without resolving these issues. TSA officials stated that they deployed the ETPs to respond quickly to the threat posed by a potential suicide bomber after suicide bombings had been carried out onboard Russian airliners in 2004. TSA officials stated that they plan to continue to use the 90 ETPs currently deployed to airports. Because the ETPs were deployed without resolving their performance problems and validating all of the functional requirements, the ETPs have not been demonstrated to increase security at the checkpoint. In the future, using validated technologies would enhance TSA's efforts to improve checkpoint security.



S&T and TSA Investments in RDT&E Resulted in the Procurement or Deployment of Six New Checkpoint Technologies



As a result of S&T and TSA investments in the RDT&E of checkpoint screening technologies since TSA's creation in 2001, six new screening technologies are being procured and/or deployed, while four checkpoint screening technologies are currently in the research and development phase.⁴⁴ Based on S&T and TSA RDT&E efforts, the agency has initiated deployments of four technologies—the ETP, Fido PaxPoint Bottled Liquids Scanner, Advanced Technology Systems, and Cast and Prosthesis Scanner—three of which originated as commercial-off-the-shelf technologies or commercial-off-the-shelf technologies that TSA modified for use as checkpoint screening devices.⁴⁵ However, TSA has not completed the deployment for all of these four technologies to airports nationwide. TSA officials stated that they did not deploy additional checkpoint screening technologies because they were primarily focused on deploying explosives detection systems to screen checked baggage, as mandated by ATSA. TSA has also initiated procurements of two additional technologies—Automated Explosives Detection System for Carry-on Baggage and Whole Body Imager—but has not deployed either of them yet. Figure 3 describes the status of the six checkpoint screening technologies for which TSA has initiated procurement and/or deployment.

⁴⁴Some of the technologies that have initiated deployments or procurements are continuing in research and development to do follow-on work. For example, the Bottled Liquids Scanner and Advanced Technology Systems continue to be enhanced.

⁴⁵Commercial-off-the-shelf technology is a product or service that has been developed for sale, lease, or license to the general public and is currently available at a fair market value. The product or service can sometimes be modified, which can save time and money compared to researching, developing, and producing a product from scratch.



Figure 3: Status of Six Checkpoint Screening Technologies that Had Initiated Procurement and/or Deployment as of September 2008

Technology	Description	Status of		
		Operational Testing	Procurement	Deployment to Airports
<p>Explosives Trace Portal (ETP)</p>  <p>Source: GAO.</p>	<p>Detects traces of explosives on a passenger by using puffs of air to dislodge particles from the passenger's body and clothing that the machine analyzes for traces of explosives. Used for secondary screening.</p>	<p>Completed for earlier models, but not for models ultimately deployed. We discuss this in more detail later in the report.</p>	<p>TSA procured 207 ETPs. In June 2006, TSA halted further procurement due to high installation and maintenance costs and performance issues. One hundred and sixteen of the procured units remain in storage.</p>	<p>TSA deployed 101 portals to 36 airports during fiscal years 2005 and 2006. In June 2006, TSA halted further deployment due to performance, maintenance, and installation issues. Since June 2006, TSA has removed 11 ETPs from airports due to maintenance issues and placed them in a warehouse for storage.</p>
<p>Bottled Liquids Scanner</p>  <p>Source: ICx Technologies, Inc.</p>	<p>Hand-held or table-top units that screen for liquid explosives by detecting vapors of certain chemicals. Used for secondary screening.</p>	<p>Completed for ICx Nomadics Fido PaxPoint model, which is a type of hand-held device. Laboratory and operational tests are ongoing for hand-held and/or table-top Bottled Liquids Scanner devices.</p>	<p>TSA procured 215 Fido PaxPoint units during fiscal year 2007 and 79 Smiths Detection Sabre 4000 units during fiscal years 2007 and 2008. TSA planned to procure up to 750 hand-held and/or table-top units in late fiscal year 2008. TSA increased its planned procurement for fiscal year 2008 as a result of supplemental appropriations received in fiscal year 2007 and appropriations available in fiscal year 2008. Forty-one Smiths Detection units are at TSA headquarters or in a warehouse in case they are needed for rapid deployment.</p>	<p>TSA deployed 200 Fido PaxPoint units from July 2007 to January 2008. TSA deployed 38 Smiths Detection Sabre 4000 units from July 2007 through December 2007, and 30 units are currently in the process of being deployed. TSA plans to deploy a total of 1,300 units at all category X through category IV airports. Full operating capability is planned for fiscal year 2011.</p>

Technology	Description	Status of		
		Operational Testing	Procurement	Deployment to Airports
 <p>Advanced Technology Systems</p>	<p>Intended to improve capability to detect threat items, such as explosives. The units will replace the Threat Image Projection Ready X-ray machines used at airports for primary screening of carry-on items.</p>	<p>Completed</p>	<p>TSA procured 250 units during fiscal year 2007. Due to the availability of supplemental funding, appropriations available in fiscal year 2008, and the need to expedite procurement of these systems, the fiscal year 2008 planned procurement was 582 units, of which 250 units have been procured. In fiscal year 2009, TSA plans to award a contract to enhance current units.</p>	<p>From April 2008 to June 2008, 204 units were deployed to 12 airports, and about 287 additional units were planned to be deployed by the end of fiscal year 2008. For units deployed in fiscal year 2008, TSA plans to upgrade them in the field to incorporate the enhancements under the contract to be awarded in fiscal year 2009. TSA plans to deploy up to a total of 2,325 units at every checkpoint lane in all category X through category IV airports. Full operating capability is planned for fiscal year 2014.</p>
 <p>Cast and Prosthesis Scanner</p>	<p>Provides a two-dimensional image of the area beneath a cast or inside a prosthetic device. The device operates similarly to the whole body imager, but for localized regions of a passenger's body. Intended for use as a secondary screening device.</p>	<p>Completed</p>	<p>TSA procured 34 units during fiscal year 2007. Planned procurement was reduced from 40 to 34 units due to a system maintenance cost increase. Due to a change in priorities, planned procurement of 75 units in fiscal year 2008 was cancelled because funds were redirected to procure additional units of Advanced Technology Systems and Whole Body Imagers. TSA has no plans to procure additional units in the future.</p>	<p>Deployment of 34 units to 10 airports began in July 2008 with the deployment of 5 units; the remaining units were expected to be deployed by the end of September 2008.</p>

Source: Rapiscan Systems, Inc. © 2009.

Source: CastScopeTM.

Technology	Description	Status of		
		Operational Testing	Procurement	Deployment to Airports
<p>Automated Explosives Detection System for Carry-on Baggage^b</p> 	<p>Creates a three-dimensional image of carry-on items to detect explosives and non-metallic weapons. Being considered as a secondary screening device.^c</p>	<p>Expected to be completed in September 2009.</p>	<p>TSA procured 20 units during fiscal year 2007 for operational testing. TSA had no plans to procure any units in fiscal year 2008.</p>	<p>Deployment to checkpoints at category III and IV airports is expected to begin after operational testing has been completed in September 2009.</p>
<p>Whole Body Imager</p> 	<p>Scans passengers by producing a two-dimensional, full-body computer-generated image that reveals object anomalies underneath clothing, including plastic explosives and concealed metallic, non-metallic, ceramic and plastic objects. TSA is evaluating the feasibility of using this system as a primary and secondary screening device.^d</p>	<p>Expected to be completed in fiscal year 2009.</p>	<p>TSA leased 15 units in fiscal year 2007 for operational testing. Due to the availability of fiscal year 2008 appropriations, 135 units were planned for procurement in fiscal year 2008, of which 47 have been procured. In fiscal year 2009, TSA plans to award a contract for enhanced units.</p>	<p>Deployment of 150 units is expected to begin in fiscal year 2010. For units deployed in fiscal year 2008 for testing, TSA plans to upgrade them in the field to incorporate the enhancements under the contract to be awarded in fiscal year 2009. TSA plans to deploy a total of 878 units at all category X through category IV airports. Full operating capability is expected in fiscal year 2014.</p>

Source: Analogic Corporation.

Source: American Science & Engineering, Inc. © 2006.

Source: TSA and S&T.

^aTSA classifies the commercial airports in the United States into one of five security risk categories (X, I, II, III, and IV). In general, category X airports have the largest number of passenger boardings, and category IV airports have the smallest. Categories X, I, II, and III airports account for more than 90 percent of the nation's air traffic.

^bAlthough this technology has an automated detection capability, TSA is not testing the automated detection function in an operational environment.

^cResearch and development of this technology is continuing, specifically, to develop a computed tomography (CT) X-ray for carry-on baggage. This technology will permit fully-automated inspection of passenger baggage as opposed to the TSA screeners having to interpret the results of the baggage screening process. Operational testing of the CT X-ray technology is to be completed in fiscal year 2009.

⁴⁵Research and development of this technology is continuing, specifically, to develop passive terahertz (THz) and active gigahertz (GHz) technologies to improve detection performance and reduce operational costs of commercially available systems. Operational testing of the THz and GHz technologies is to be completed in fiscal years 2009 and 2010, respectively.

According to TSA's August 2008 strategic plan for checkpoint technologies, there are several other ongoing efforts in addition to the technologies discussed in figure 3.⁴⁶ S&T and TSA are researching and developing a shoe scanning device that is to conduct automated weapons and explosive detection without requiring passengers to remove their footwear. TSA plans to award a contract in fiscal year 2010, with full operating capability in fiscal year 2015. TSA plans to deploy 1,300 units at all category X through category IV airports. TSA also has two ongoing efforts related to boarding pass and credential authentication, according to the agency's strategic plan. Starting in 2007, TSA assumed responsibility from airline contractors for travel document checking, which is currently conducted manually. TSA plans to replace the manual system with an automated one. Specifically, the Boarding Pass Scanning System is expected to verify the authenticity of a boarding pass at the checkpoint and enable the use of paperless boarding passes by the airlines. In addition, the Credential Authentication Technology System is planned to be an automated system that authenticates identification presented by passengers and airport employees. According to TSA, the agency plans to eventually combine both of these authentication systems in a single travel document checking system. TSA plans to award a contract for these two systems in fiscal year 2009, with full operating capability expected in fiscal year 2014. TSA plans to deploy a total of 878 units to replace the existing document verification tools at all category X through category IV airports. Another ongoing effort identified in TSA's strategic plan is the Next Generation ETD. This system is planned to replace legacy ETD systems and to be able to identify a larger range of explosives. Specifically, this system is expected to have enhanced explosive detection capability in terms of sensitivity and the ability to detect new threats, as well as other improvements over legacy systems, which are expected to produce lower lifecycle costs. TSA plans to deploy 1,500 units at all category X through category IV airports.

⁴⁶TSA submitted a strategic plan for the PSP to congressional committees in September 2008. In the plan TSA identified several new technologies that the agency had not previously identified to us. Because we did not receive this strategic plan until toward the end of our review in September 2008, we did not conduct detailed assessments of these particular technologies.

TSA also has two additional efforts to assess possible technologies. One effort is called Standoff Detection, which is intended to display images to detect anomalies concealed under passengers' clothing. TSA plans to conduct an operational utility evaluation of test article units during fiscal year 2009 to evaluate the technology's feasibility within checkpoint screening operations. According to TSA, this technology would assist the agency in applying layered security prior to the checkpoint in soft target areas, such as airport lobbies, to improve early awareness of a potential explosive threat. If the technology proves effective in the checkpoint operation, TSA plans to award a contract in fiscal year 2010, with full operational capability expected by fiscal year 2014, and to deploy 351 units to every checkpoint at category X and category I airports. The other effort is called Explosives Characterization for Trace (Chemical-based) Detection. This effort includes the research and development of trace signatures, detection, and physical properties of explosives to improve the detection and performance of deployed explosives trace detection technologies.

TSA Procured and Deployed ETPs without Assurance that They Would Perform as Intended in an Operational Setting

During 2004 and 2005, prior to deployment of the ETPs, TSA conducted a series of acceptance tests (that is, laboratory tests) of the General Electric and Smiths Detection ETPs that suggested they had not demonstrated reliable performance. Specifically, in 2004, TSA conducted acceptance tests on early models of the General Electric and Smiths Detection ETPs to determine whether the ETPs met key functional requirements. Subsequently, in 2004 a General Electric ETP model was field tested at five airports to determine how well the ETP performed in an operational environment. A Smiths Detection ETP model was also field tested at an airport in 2004. Based on initial test results, both vendors of the ETPs modified the machines, and TSA conducted further laboratory testing. The modified General Electric ETP was tested from December 2004 through February 2005. During the January 2005 to May 2005 time frame, both the General Electric and Smiths Detection ETP models were tested. Even though tests conducted during 2004 and 2005 of the General Electric and Smiths Detection ETPs suggested they had not demonstrated reliable performance, TSA deployed the Smiths Detection ETP and General

Electric ETP to airports starting in July 2005 and January 2006, respectively, without resolving identified performance issues.⁴⁷

Further, TSA did not test all 157 of the ETP's functional requirements prior to procuring and deploying the General Electric and Smiths Detection ETP models. Instead, TSA tested the ETP models against a subset of the functional requirements. According to TSA's System Development Life Cycle Guidance, testing of a system is to be conducted to prove that the developed system satisfies its requirements in the functional requirements document. TSA officials could not identify the specific requirements that were tested or the reason(s) that all of the requirements were not tested.

A TSA official stated that TSA had intended to resolve problems regarding the ETPs' performance after they had been deployed, but TSA officials could not explain how these problems were to be resolved. Officials further stated that they worked for over 1 year during 2006 and 2007 with the ETP vendors to correct reliability and maintenance issues after the ETPs were initially deployed, but could not resolve them. Furthermore, according to S&T officials, when TSA conducted limited field tests, the ETP manufacturers provided different configurations from those used during the laboratory tests. According to officials, once this was discovered, it took more than 6 months for the ETP manufacturers to recreate the configurations that had passed the laboratory tests. TSA officials stated that, during this 6-month period, the agency decided to award a sole source contract to General Electric to procure its ETP.

Regarding the reliability of the ETPs, of the 101 ETPs (71 from General Electric and 30 from Smiths Detection) that were originally deployed to 36 airports, the General Electric ETP did not meet the system requirement for operational availability due to frequent breakdowns. Both vendors' ETPs were also more expensive to maintain than expected, according to the TSA Chief Technology Officer serving during this period. The functional requirements document requires the ETP to be operationally available 98.38 percent of the time. However, the General Electric ETPs were not always able to meet this requirement. TSA officials could not provide information on the operational availability of the Smiths Detection ETPs. For the General Electric ETPs, from January through May 2006, they were

⁴⁷According to TSA, the specific methods and results of testing of the ETPs during the research and development phase are sensitive security information protected from disclosure pursuant to 49 C.F.R. § 1520.5(b). As a result, the relevant sections are described in the restricted version of this report.

operationally available an average of 98.05 percent of the time, although the ETPs met the operational availability requirement for 2 months during that period. Furthermore, TSA's operational requirements specify that the ETP should function for a minimum of 1,460 hours between critical failures. A critical failure means that an ETP fails to operate and must be repaired as soon as possible. However, the TSA Chief Technology Officer at the time stated that the ETPs operated at a much lower average number of hours before a critical failure occurred because, for example, the dirt and humidity of some airport environments adversely affected the equipment. Specifically, from January 2006 through May 2006, the General Electric ETPs operated for an average of 559 hours before a critical failure, which means that these ETPs operated on average 38 percent of the time that they were required to operate before a critical failure occurred. TSA officials could not provide information on the mean time between critical failures for the Smiths Detection ETPs. TSA officials stated that they tested the ETPs in several airports for several months prior to deployment, but data from these tests did not identify a problem with mean time between critical failures. One reason for this, a TSA official stated, was that not enough data were collected during the field tests. As usage of the ETPs increased, officials stated that they discovered the ETP was not meeting operational availability requirements. The ETPs also required replacement filters and other consumables more often than expected, according to officials, which drove up maintenance costs.

According to TSA officials, because of a variance in operational availability hours among the deployed ETPs, maintenance problems, and the high cost of ETP installation at airports, in June 2006, the agency halted the deployment of the ETP to additional airports and stopped the planned purchase of additional ETPs. TSA officials plan to continue to use the 90 ETPs currently deployed to airports. However, without validating that the ETPs meet their functional requirements, TSA officials do not have assurance that it is worthwhile to continue to use the ETPs in light of the cost to maintain and operate them. In addition, TSA officials are considering what to do with the ETPs that were procured and are currently in storage. As of April 2009, 116 ETPs were in storage.⁴⁸

⁴⁸TSA originally deployed 101 ETPs to airport checkpoints, and had 90 ETPs at airports and 116 ETPs in storage at the time we issued our restricted April 2009 report. After issuance of our restricted report, TSA stated that 22 ETPs were at airports and no ETPs were in storage as of September 2009.

TSA did not follow the Acquisition Management System (AMS) guidance or a knowledge-based acquisition approach before procuring the ETPs, which contributed to the ETPs not performing as required after they were deployed to airports. Specifically, AMS guidance provides that testing should be conducted in an operational environment to validate that the system meets all functional requirements before deployment. In addition, our reviews have shown that leading commercial firms follow a knowledge-based approach to major acquisitions and do not proceed with large investments unless the product's design demonstrates its ability to meet functional requirements and be stable.⁴⁹ The developer must show that the product can be manufactured within cost, schedule, and quality targets and is reliable before production begins and the system is used in day-to-day operations. As discussed earlier in this report, TSA officials told us that they deployed the ETP despite performance problems because officials wanted to quickly respond to emergent threats. However, TSA did not provide written documentation to us that described the process used at the time to make the decision to deploy the ETP or the process that is currently used to make deployment decisions.

Using Validated Technologies Would Enhance TSA's Efforts to Improve Checkpoint Security

TSA has relied on technologies in day-to-day airport operations that have not been demonstrated to meet their functional requirements in an operational environment. For example, TSA has substituted existing screening procedures with screening by the Whole Body Imager even though its performance has not yet been validated by testing in an operational environment. In the future, using validated technologies would enhance TSA's efforts to improve checkpoint security. Furthermore, without retaining existing screening procedures until the effectiveness of future technologies has been validated, TSA officials cannot be sure that checkpoint security will be improved.⁵⁰

⁴⁹GAO, *Best Practices: Using a Knowledge-Based Approach to Improve Weapon Acquisition*, GAO-04-386SP (Washington, D.C.: January 2004).

⁵⁰According to TSA, our evaluation of TSA's use and validation of airport screening technologies is sensitive security information protected from disclosure pursuant to 49 C.F.R. § 1520.5(b)(9)(v). As a result, the relevant sections are described in the restricted version of this report.

DHS Is Addressing Coordination and Collaboration Challenges with Stakeholders to Research, Develop, and Deploy Checkpoint Screening Technologies

DHS S&T and TSA coordinated and collaborated with each other and key stakeholders on their research, development, and deployment activities for airport checkpoint screening technologies, and DHS is taking actions to address challenges and strengthen these efforts.⁵¹ Because S&T and TSA share responsibilities related to the RDT&E, procurement, and deployment of checkpoint screening technologies, the two organizations must coordinate with each other and external stakeholders, such as airport operators and technology vendors. For example, in accordance with provisions of the Homeland Security Act and ATSA, S&T and TSA are to coordinate and collaborate with internal and external stakeholders on matters related to technologies and countermeasures for homeland security missions. S&T and TSA signed an MOU in August 2006 that establishes a framework to coordinate their work at the TSL, which tests and evaluates technologies under development. S&T also established a Capstone IPT for Explosives Prevention in 2006 to bring S&T, TSA, and U.S. Secret Service leadership together to identify gaps in explosives detection capability; prioritize identified gaps; review relevant, ongoing S&T programs; and develop capabilities to meet identified needs. However, inconsistent communication and the lack of an overarching test and evaluation strategy have limited S&T's and TSA's ability to coordinate effectively with one another. To coordinate with the aviation community, S&T and TSA have hosted industry days and conference calls to discuss new technologies with airport operators and technology vendors. Although TSA has taken actions to build partnerships with airport operators and vendors, it has not established a systematic process to coordinate with them related to checkpoint screening technologies. However, TSA officials stated that they are in the beginning stages of establishing a systematic process.

⁵¹S&T is responsible for conducting basic and applied research, and advanced development, including developmental test and evaluation. TSA is responsible for conducting operational test and evaluation, operational integration, procurement and deployment of new technologies, including checkpoint screening technologies.

S&T and TSA Are Addressing Coordination and Collaboration Challenges with Each Other on New Checkpoint Screening Technologies, but Challenges Remain

S&T and TSA have taken actions to coordinate and collaborate with each other related to the RDT&E of checkpoint screening technologies, such as by communicating priorities and requirements for technologies and working with each other on the Capstone IPT for Explosives Prevention. However, S&T and TSA coordination and collaboration were not always effective due to inconsistent communication and the lack of an overarching test and evaluation strategy. The Homeland Security Act assigned responsibilities within the department for coordinating and integrating the research, development, demonstration, testing, and evaluation activities of the department, as well as for working with federal and private sector stakeholders to develop innovative approaches to produce and deploy the best available technologies for homeland security missions. The act further assigned S&T with responsibility for coordinating with other appropriate executive agencies in developing and carrying out the science and technology agenda of the department to reduce duplication and identify unmet needs. ATSA had also assigned TSA with coordination responsibilities, including the coordination of countermeasures with appropriate departments, agencies, and instrumentalities of the U.S. government.⁵²

S&T and TSA have taken several actions to coordinate and collaborate on their research and development activities related to checkpoint screening technologies. First, to coordinate the transition of the TSL from TSA to S&T, minimize disruption of work, and prevent duplication of effort, S&T and TSA signed an MOU that defines the roles and responsibilities for the research and development of homeland security technologies, including checkpoint screening, and establishes a framework for how to coordinate their work. Additionally, S&T created the Capstone IPT for Explosives Prevention, which is co-chaired by the Assistant Secretary for TSA and the Director of the U.S. Secret Service, to identify and prioritize capabilities needed to detect explosives; review relevant, ongoing S&T programs; and develop capabilities to meet the identified needs. The IPT was first convened in December 2006 to identify research and development priorities for explosives detection technologies at airport checkpoints as

⁵²In accordance with provisions of the Homeland Security Act and ATSA, the S&T's Explosives Division and TSA should coordinate with one another and other stakeholders, including the commercial aviation community and DHS components, to facilitate the research, development, and deployment of checkpoint screening technologies. TSA should also coordinate countermeasures to protect civil aviation with appropriate federal departments and agencies. See 49 U.S.C. § 114(f)(4). The S&T Explosives Division develops technical capabilities to detect, interdict, and lessen impacts of nonnuclear explosives used in terrorist attacks against mass transit, civil aviation, and critical infrastructure.

well as for other transportation modes, and has met periodically since then. According to TSA officials, the Capstone IPT has enabled TSA to establish a clear understanding with S&T of TSA's needs for technology solutions that meet stringent detection thresholds and throughput requirements to support the aviation sector. Additionally, the officials stated that the Capstone IPT has given TSA a better collective understanding of the technology needs of other DHS components, which will help DHS identify technology solutions that can be combined to benefit multiple users. Finally, to follow through on the priorities established by the Capstone IPT for Explosives Prevention, S&T officials stated that they established project-level IPTs, including one for airport checkpoints and one for homemade explosives. S&T officials stated that they are working with TSA on these project-level IPTs to try to meet the needs identified by the Capstone IPT. TSA officials further stated that they have PSP IPTs or working groups to coordinate on technology projects, establish program goals and objectives, and develop requirements and time lines. These groups meet on a weekly basis, according to TSA officials. In April 2008, S&T dissolved the IPT for explosives detection and replaced it with two separate IPTs, a transportation security IPT, chaired by TSA and a counter-IED IPT, chaired by the Office of Bombing Prevention within the National Protection and Programs Directorate and the United States Secret Service.

Coordination and collaboration efforts between S&T and TSA have helped in identifying checkpoint screening solutions. For example, S&T and TSA officials collaborated on a hand-held vapor detection unit called the Fido PaxPoint. After the August 2006, discovery of the alleged plot to detonate liquid explosives on board commercial air carriers bound for the United States from the United Kingdom, S&T and TSA worked together to identify, develop, and test screening technologies to address this threat. According to TSA officials, S&T learned that the Department of Defense had developed a handheld unit that could detect vapors from explosives. S&T modified the Department of Defense handheld unit, resulting in the Fido PaxPoint unit to screen liquids and gels at airport checkpoints for explosives, and S&T helped TSA test and evaluate the device.⁵³

⁵³Even though TSA officials stated that the Fido PaxPoint was determined to be effective, the data collection process for it has been extended to ascertain its operational suitability, specifically, how sustainable and maintainable it is. TSA could not provide information to us on the status of this data collection process.

Although S&T and TSA have taken steps to coordinate and collaborate with one another, inconsistent communication and a lack of an overarching test and evaluation strategy have contributed to coordination and collaboration challenges. Specifically, communication between S&T and TSA related to S&T's basic and applied research efforts and TSA's efforts to modify commercially available technologies has been lacking at times. For example, TSA officials stated that early in the TSL's transition to S&T (that is, during fiscal year 2006), TSA did not receive information from S&T regarding which of TSA's research and development needs S&T would fund, which projects related to airport checkpoint technologies were underway at the TSL, or the time frames to complete those projects. TSA officials stated that, without this information, TSA was unable to determine whether its work on modifying commercially available technologies for screening passengers and carry-on items unnecessarily duplicated S&T's research and development efforts, although TSA officials were not aware of any duplication that occurred. An S&T official further stated that TSA had not consistently fulfilled its responsibility to provide clearly defined functional requirements for the equipment to be developed by S&T and tested by the TSL, nor has TSA consistently given sufficient notice to the TSL of TSA testing requests. Under the S&T and TSA MOU, TSA has retained responsibility to establish requirements for equipment certification and qualification and acceptance testing. Specifically, an S&T official at the TSL stated that TSA had inadequately defined the functional requirements and allowed too little time for testing several checkpoint screening technologies, including the Advanced Technology Systems, Enhanced Metal Detector II, and Bottled Liquids Scanner. A TSL official acknowledged that when the TSA was responsible for the TSL, the agency had not consistently developed requirements prior to testing or certification of equipment as required by the DHS guidance.⁵⁴

In another example, as previously mentioned in this report, TSA is developing new certification standards and functional requirements for screening technologies, and is working with national laboratories to validate data on aircraft vulnerabilities and generate new computer models to help TSA develop requirements for explosives detection. According to the TSA Chief Technology Officer in 2007, the TSL has custody of the aircraft vulnerability data, but TSL officials had refused to release the data to the national laboratories as requested by TSA. Although

⁵⁴DHS Investment Review Process Management Directive 1400. This directive was replaced in November 2008 by an Interim Acquisition Directive (102-01).

the TSL later provided 32 of the 46 requested reports, TSA officials estimated that the TSL's refusal to release all of the reports had delayed the effort to develop new certification standards and technology requirements by about 1 month. The officials added that most of TSA's requests to S&T and the TSL had involved similar problems and that, although the MOU provides a framework for coordination, these types of problems are related to day-to-day operations and will have to be resolved as situations arise.

According to S&T and TSA officials, senior-level management turnover at S&T and TSA contributed to these communication difficulties, as well as an S&T reorganization which began in August 2006 with the arrival of a new Under Secretary for Science and Technology. S&T officials further stated that, prior to the establishment of the PSP working groups, there was no mechanism for S&T and TSA to communicate information about priorities, funding, or project timelines. However, through the working groups, S&T officials stated that S&T and TSA are beginning to achieve regular communication and interaction at the working level, which allows for information to be shared in a mutually beneficial way. S&T and TSA officials also stated that communication with each other has improved since the MOU was signed in August 2006 and, in particular since the summer of 2007, although officials from both organizations stated that further improvement is needed. According to S&T officials, the TSL's independent test and evaluation division and TSA have developed an effective working relationship for several programs, including the Whole Body Imager and Advanced Technology Systems. In addition, S&T officials stated that TSA has come to better understand the processes involving the Capstone IPT and identifying capability needs. According to TSA officials, the agency is in the process of determining whether a position within its Office of Security Technology should be established as a liaison with S&T to improve coordination between S&T and TSA. If the position is created, the TSA liaison would coordinate and collaborate with S&T officials on technology projects by assessing the science that supports the technologies.

The MOU specifies that S&T and TSA will coordinate activities, including developing an integrated, overarching test and evaluation strategy for projects to ensure that test and evaluation functions are not duplicative, adequate resources are outlined and secured for these functions, and activities are scheduled to support the overall project master schedule. However, an overarching test and evaluation strategy for checkpoint technologies has not been developed. The lack of this strategy has presented coordination and collaboration challenges between S&T and

TSA, and has resulted in the delay of some technologies. For example, a TSL official stated that the TSL could not accommodate TSA's request to test the Advanced Technology Systems, in part, because TSA officials had not provided sufficient advance notice of their testing needs. TSA officials said they were working with S&T to develop a project master schedule for the Advanced Technology Systems. S&T and TSA officials stated that they plan to develop a test and evaluation strategy to define a coordinated technology transition process from S&T to TSA by outlining key responsibilities and criteria to initiate field evaluations of technologies, but officials could not tell us when the test and evaluation strategy would be completed.

DHS Is Using Several Approaches to Strengthen Coordination and Collaboration with Airport Operators, Technology Vendors, and Other Federal Agencies

DHS, through S&T and TSA, coordinates with airport operators, private sector partners, such as technology vendors, and other federal agencies on matters related to research and development efforts. This coordination and collaboration between TSA and airport operators and technology vendors is important because the agency relies on airport operators to facilitate the deployment of equipment for testing and day-to-day operations, and on vendors to develop and manufacture new screening equipment.⁵⁵ However, TSA does not have a systematic process to coordinate with external stakeholders related to checkpoint screening technologies, but TSA officials stated that the agency has developed a draft communications plan, which is being reviewed.

Although TSA does not have a systematic process to coordinate with technology vendors, airport operators, and other stakeholders related to the RDT&E, procurement, and deployment of checkpoint screening technologies, agency officials stated that they plan to develop and implement such a process. Specifically, TSA officials stated that they have developed a draft communications plan, which is being reviewed, that will document the communications process. However, TSA could not provide an expected completion date for the plan. Although such a plan should help in providing consistency to the agency's coordination efforts, without knowing the specific activities the plan will include or when it will be implemented, we cannot determine the extent to which the plan may

⁵⁵We focused our work on TSA's coordination and collaboration with airport operators and technology vendors, and not on S&T's coordination and collaboration with these external stakeholders, because TSA is responsible for procuring and deploying checkpoint technologies.

strengthen coordination. In addition, in September 2007, TSA hired an Industry Outreach Manager within its Office of Security Technology to improve relationships with airport operators and communication with internal TSA stakeholders related to screening technologies, including checkpoint technologies. In general, the Industry Outreach Manager is the communications liaison for the Office of Security Technology stakeholders and customers to exchange ideas, information, and operational expertise in support of the office's mission and goals, and to provide cutting-edge technologies in the most efficient and cost-effective means possible. In addition to these steps, in January 2007, S&T created a Corporate Communications Division to coordinate on a wide variety of science and technology efforts with public and private sector stakeholders. This office is in the process of developing a tool to assess the effectiveness of its outreach efforts to industry stakeholders.

The AMS guidance recommends that TSA coordinate with airport operators to work out all equipment installation issues prior to deployment. According to TSA officials, the role of the airport operator is essential in ensuring that solutions under development are suitable for use in an airport environment, taking into consideration all logistical and operational constraints and possibilities. As described earlier, provisions of the Homeland Security Act address the need to coordinate research and development efforts to further homeland security missions, and reinforce the importance of coordinating and collaborating with airport operators. TSA sponsors monthly conference calls with airport operators to discuss issues of general interest and, according to S&T officials, S&T has conducted pilot studies with airport operators. However, according to many of the 33 airport operators we interviewed,⁵⁶ TSA's coordination on the priorities for and deployment of checkpoint screening technologies has been inconsistent. Specifically, of the 33 airport operators we interviewed, 8 had only positive comments about TSA's coordination and 16 expressed only concerns regarding TSA's coordination efforts, while 9 expressed both positive comments and concerns. Eleven of the 33 airport operators told us that TSA had not shared information with them regarding checkpoint technology needs and priorities. For example, an airport operator stated that TSA provided specifications for new screening technologies with sufficient lead time for the airport, which was building a

⁵⁶We selected a nonprobability sample of 40 airports and obtained the views of 46 operators at these airports regarding coordination with TSA. Thirteen of the 46 airport operators did not express an opinion about coordination for and deployment of checkpoint screening technologies. See appendix I for more information on how we selected these airports.

new checkpoint at the time, and that TSA had numerous coordination meetings with airport officials to determine space constraints, power requirements, and other factors. However, this same airport operator expressed a desire for more coordination by TSA in the agency's selection of the technologies to be pilot tested at this airport. Another airport operator stated that, when TSA asks for volunteers to participate in checkpoint screening technology pilot programs, it is difficult to agree to participate because TSA does not clearly communicate the program's goals or the capabilities of the technology in the pilot program.

According to airport operators at another airport, TSA officials told them that they would have the latitude to select the ETP from either of two vendors on the TSA contract for purchase. According to the airport officials, after they selected equipment from one of the vendors because it would fit into the physical layout of the airport's checkpoint, TSA told the airport officials that particular ETP vendor was no longer under contract with TSA. As a result, airport officials stated that they had to redesign the checkpoint, including raising the ceiling, to accommodate the other vendor's ETP. Senior officials in TSA's Office of Operational Process and Technology, the office responsible for the development and implementation of security technologies across several modes of transportation, subsequently agreed that coordination with airport managers and other stakeholders could be improved.

According to TSA officials, coordinating with technology vendors is essential in order to determine what technology platform would be appropriate and capable of providing the required detection and throughput capabilities. S&T and TSA have conducted outreach efforts to coordinate with technology vendors. For example, S&T officials stated that they have hosted forums known as industry days and attended conferences to discuss types of technologies needed to be developed and the department's priorities for research and development. S&T officials also stated that they make presentations at technology-related conferences, symposia, and exhibits, highlighting the work conducted by S&T. At every industry day and conference, officials said, airport security and checkpoint screening technologies have been discussed. In addition, TSA has coordinated with technology vendors through industry days, individual meetings, and conferences. For example, TSA officials stated that TSA held industry days with technology vendors to provide a forum to communicate information to potential vendors on specific technology testing and procurement efforts, and to allow vendors to ask questions regarding technology projects and TSA expectations.

Despite these outreach efforts, of the seven vendors we interviewed who had contracted with TSA to provide checkpoint screening technologies, officials from five vendors expressed concerns about the agency's ability to coordinate with them on current or future needs for checkpoint technologies. Officials from four of the seven vendors stated that TSA had not communicated a strategic vision for screening technologies that will be needed at the checkpoint in the future, and that TSA did not effectively and clearly communicate standards and requirements for technologies to vendors. For example, just as TSL officials commented that TSA did not always provide clear and quantifiable requirements to conduct tests of screening technologies, vendors stated that TSA had not communicated effectively about its future needs, such as the operational requirements for an advanced, integrated checkpoint screening system.⁵⁷ Therefore, a vendor official stated that some of them had taken the initiative to develop integrated screening technologies in the hope that TSA will eventually request this type of integrated system. TSA did not express an opinion regarding the specific concerns raised by the technology vendors, but a senior TSL official stated that TSA should sponsor better briefings for vendors after the agency announces its intentions to develop new technologies. The official stated that these briefings could provide vendors with an opportunity for open dialogue with TSA and clarification of TSA's needs for new technologies. According to a vendor, without adequate coordination and communication from TSA, the vendors' ability is limited in deciding how best to invest their resources to develop new checkpoint screening technologies.

In addition to coordinating and collaborating with airport operators and technology vendors, S&T and TSA coordinate and collaborate on the department's RDT&E efforts with other federal agencies through participation in the Technical Support Working Group, which is co-chaired by the Departments of Defense and State. The Technical Support Working Group is the U.S. national forum that identifies, prioritizes, and coordinates interagency research and development of technologies to

⁵⁷Section 4014 of the Intelligence Reform Act required TSA to "develop and initiate a pilot program to deploy and test advanced airport checkpoint screening devices and technology as an integrated system at not less than 5 airports in the United States" by March 31, 2005. See Pub. L. No. 108-458, § 4014, 118 Stat. at 3720. According to TSA, the only advanced checkpoint screening technology available to TSA at that time was the ETP, and TSA initially conducted pilot tests at five airports and later expanded the tests to 16 airports. TSA officials stated that the agency submitted a strategic report to Congress on August 9, 2005, *Detection Equipment at Airport Screening Checkpoints*, in satisfaction of this requirement in the Act.

combat terrorist acts, including explosives detection technologies. S&T also coordinates with the national laboratories on homeland security research.⁵⁸ Specifically, S&T's Office of National Laboratories coordinates homeland security-related activities and laboratory-directed research conducted within the Department of Energy's national laboratories. According to an S&T senior official, S&T has worked with the national laboratories to supplement S&T's research and development of explosives detection technologies by tasking the national laboratories to conduct basic research on the characteristics of homemade explosives.

Conclusions

Researching, developing, testing and evaluating, procuring, and deploying checkpoint technologies capable of detecting ever-changing threats to the commercial aviation system is a daunting task. Although TSA has recently produced a strategic plan that identified a strategy for the PSP, neither the plan nor the agency's strategy for researching, developing, and deploying checkpoint technologies was informed by some key risk management principles, including a risk assessment, cost-benefit analysis, and performance measures. Without conducting a risk assessment that includes all three elements of risk—threat, vulnerability, and consequence—and completing a cost-benefit analysis to guide the PSP strategy, TSA has limited assurance that its strategy targets the most critical risks and that it invests in the most cost-effective new technologies or other protective measures. Further, without developing performance measures that assess the extent to which checkpoint screening technologies achieve the PSP's security goals and thereby reduce or mitigate the risk of terrorist attacks, TSA is limited in its ability to determine the success of its strategy and make needed adjustments. Even though TSA has not implemented a risk-informed strategy to ensure that its investments target the most pressing security needs, the agency has moved forward in investing in new checkpoint screening technologies.

Despite limited progress in the RDT&E, procurement, and deployment of new checkpoint screening technologies during the first few years that S&T and TSA had responsibilities related to these technologies, more recently, the organizations have made progress as reflected by the number of technologies for which procurement and deployment has been initiated.

⁵⁸The Homeland Security Act addresses the need for DHS to work with federal laboratories and the private sector, among others, to develop innovative approaches to produce and deploy the best available technologies for homeland security missions. See Pub. L. No. 107-296, § 102(f)(5), 116 Stat. at 2143-44.

TSA faced challenges with the first new technology that it procured and deployed—the ETP. In the interest of protecting the homeland, it is understandable that TSA may, at times, not follow all established guidance in an effort to deploy technologies quickly to address urgent threats and vulnerabilities. However, deploying the ETP despite unresolved performance concerns identified during testing of earlier ETP models, as well as failing to ensure that ETP models that were ultimately deployed had passed operational testing, increased the risk that the machines would not perform as intended, resulting in a questionable security benefit. TSA did not follow AMS guidance that recommended operational testing of a new technology prior to deployment because it is more cost effective to resolve performance issues then. While TSA deployed the ETPs to provide a much-needed capability to automatically screen higher risk passengers at airport checkpoints, relying on the ETPs could have resulted in airport checkpoints being more vulnerable given the ETPs' performance problems and lack of operational testing. Also, relying on the ETPs to screen these particular passengers instead of existing screening procedures may not enhance airport checkpoint security because TSA does not know if ETP screening provides an improved detection capability compared to existing screening procedures. Moreover, it is risky to substitute any new technology for existing screening procedures before the technology has been proven to be effective through operational testing. Although TSA is trying to deploy new technologies to address immediate threats, the problems associated with the development and deployment of the ETPs may be repeated with other technologies unless TSA adheres to testing guidance and makes decisions using a knowledge-based acquisition approach. Finally, it is not clear whether it is worthwhile to continue to use the ETPs currently deployed to airports due to the costs associated with maintaining the machines in good, operational condition.

Recommendations for Executive Action

To help ensure that DHS's Science and Technology Directorate (S&T) and Transportation Security Administration (TSA) take a comprehensive, risk-informed approach to the RDT&E, procurement, and deployment of airport passenger checkpoint screening technologies, and to increase the likelihood of successful procurements and deployments of such technologies, in the restricted version of this report, we recommended that the Assistant Secretary for TSA take the following eight actions:

- Conduct a complete risk assessment, including threat, vulnerability, and consequence assessments, which would apply to the PSP.
- Develop cost-benefit analyses to assist in prioritizing investments in new checkpoint screening technologies.

-
- Develop quantifiable performance measures to assess the extent to which investments in research, development, and deployment of checkpoint screening technologies achieve performance goals for enhancing security at airport passenger checkpoints.
 - After conducting a complete risk assessment and completing cost-benefit analyses and quantifiable performance measures for the PSP, incorporate the results of these efforts into the PSP strategy as determined appropriate.
 - To the extent feasible, ensure that operational tests and evaluations have been successfully completed before deploying checkpoint screening technologies to airport checkpoints.
 - Evaluate whether TSA's current passenger screening procedures should be revised to require the use of appropriate screening procedures until it is determined that existing emerging technologies meet their functional requirements in an operational environment.
 - In the future, prior to testing or using all checkpoint screening technologies at airports, determine whether TSA's passenger screening procedures should be revised to require the use of appropriate screening procedures until the performance of the technologies has been validated through successful testing and evaluation.
 - Evaluate the benefits of the Explosives Trace Portals that are being used in airports, and compare the benefits to the costs to operate and maintain this technology to determine whether it is cost-effective to continue to use the machines in airports.

Agency Comments and Our Evaluation

We provided a draft of our restricted report to DHS for review and comment. On April 7, 2009, DHS provided written comments, which are presented in Appendix II. In commenting on our report, DHS stated that it agreed with our recommendations and identified actions planned or underway to implement them. While DHS is taking steps to address our first and second recommendations related to conducting a risk assessment, the actions DHS reported TSA had taken or plans to take do not fully address the intent of the remaining six recommendations.

In its comments, DHS stated that it concurred with our first recommendation that a risk assessment should be developed for the PSP and that TSA has two efforts currently underway to do so. Completion of TSA's first effort—the Air Domain Risk Analysis (ADRA)—is expected in the winter of 2009. DHS commented that TSA's second effort is the Risk Management and Analysis Toolset (RMAT), a model to simulate the potential of some technologies to reduce the risk of certain threat scenarios which will apply specifically to the passenger screening process. DHS reported that it expects initial results from RMAT to be available during the second quarter of 2009. DHS further stated that TSA has made

resource allocation and technology decisions that were informed by consideration of risk (including threat, vulnerability, and consequence), although not by comparative assessments of these three elements. However, as we reported, TSA has not conducted a risk assessment for the PSP, and it is unclear to what extent the ADRA would provide risk information needed to support the PSP. Until such a risk assessment is developed and integrated into TSA's strategy for the PSP, TSA continues to invest in checkpoint technologies without the benefit of a risk-informed strategy and increases the possibility that its investments will not address the highest-priority security needs.

DHS also concurred with our second recommendation that it develop cost-benefit analyses. DHS commented that TSA is developing an approach for selecting cost-effective technologies by developing life-cycle cost estimates and using the RMA tool to determine how technologies balance risk (based on current threats) with cost. TSA's decision to collect cost and benefit information is a positive first step. Irrespective of how TSA collects data on the costs and benefits of technologies, it is important, as we reported, that TSA conduct cost-benefit analysis of each checkpoint technology that it invests in that weighs the costs and benefits of technologies relative to the costs and benefits of other solutions. Such analysis is important because it helps decision-makers determine whether investments in technologies or in other security programs will provide the greatest mitigation of risk for the resources that are available.

DHS concurred with our third recommendation that TSA develop quantifiable performance measures to assess the extent to which TSA's investments in checkpoint screening technologies make the checkpoint more secure, the key mission of the program. DHS commented that it currently collects quantifiable performance attributes for all potential acquisitions with regards to metrics, such as detection, false alarm rate, and operational availability and plans to use information on machines' attributes as measures of the PSP's overall effectiveness as a program. However, these actions will not fully address our third recommendation. First, information collected on potential acquisitions prior to their deployment may not reflect their performance in an operational environment; consequently, relying on information about technologies' attributes rather than measuring the effectiveness of deployed technologies to secure the checkpoint will likely have limited value in terms of measuring the effectiveness of the PSP as a program. Second, as we reported, the ETP example illustrates that TSA did not collect information on the ETP's performance attributes such as operational availability during laboratory testing prior to procurement and did not collect data on the ETP's detection capabilities during tests in an

operational environment. This raises questions about the completeness of data TSA collects on technologies prior to acquisition and deployment. We could not verify that TSA collects such information on other technologies because TSA did not provide documentation to support this comment. As TSA moves forward in developing performance measures, it is important that these measures reflect not only efficiency of the technologies to process passengers but the effectiveness of technologies and other countermeasures to make the checkpoint more secure and thereby reduce the risks posed by those most pressing threat scenarios that will be identified once TSA completes its risk assessment.

In addition, DHS concurred with our fourth recommendation that it develop a PSP strategic plan that reflects the risk assessment, cost benefit analysis, and performance measures. DHS commented that TSA plans to combine results from the RMAT tool and lifecycle cost estimates for possible technology solutions that strike a balance between risk and efficient use of funding. DHS also stated it will use RMAT to develop proxy measures and general “what-if” analysis and risk insights. However, these actions alone will not satisfy the intent of this recommendation. While it is possible that proxy measures could be developed to assess the extent to which TSA’s investments in the research and development of technologies have achieved program goals of making the checkpoint more secure, to fully address this recommendation, TSA must also conduct a risk assessment that addresses the PSP, develop quantifiable measures that clearly assess the PSP’s progress towards its security goals, and revise its strategic plan accordingly.

DHS concurred with our fifth recommendation that before deploying technologies to airport checkpoints, the technologies should successfully complete testing and evaluation and stated that TSA is taking action to implement a formal testing process. DHS commented that TSA has prepared a Test and Evaluation Master Plan (TEMP) that describes a new formal testing process that is consistent with DHS’s new acquisition directive. However, the TEMP does not address the intent of this recommendation. We deleted from this public report our evaluation of why the TEMP does not address the intent of this recommendation, because TSA determined our evaluation to be sensitive security information.

Further, DHS agreed with our sixth and seventh recommendations that TSA evaluate whether its screening procedures should be revised to require the use of appropriate procedures until it can be determined that emerging technologies or future technologies that may be developed meet all of their requirements in an operational environment. However, DHS’s

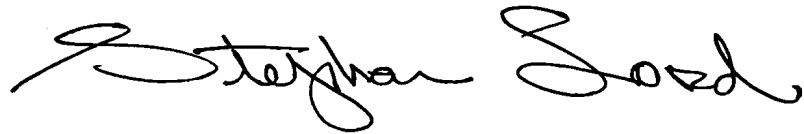
comments suggest that it does not intend to implement these recommendations. DHS commented that the performance of machines is always measured and confirmed in the laboratory setting prior to operational field testing. However, we disagree that laboratory testing is sufficient to address this recommendation. We deleted from this public report our evaluation of why laboratory testing alone does not address the intent of this recommendation, because TSA determined our evaluation to be sensitive security information.

DHS stated that TSA implemented our eighth recommendation that the agency evaluate the benefits of the ETP, such as its effectiveness, and conduct a cost-benefit analysis to determine whether the technologies should remain in use at airports. However, we disagree that TSA has implemented this recommendation. DHS commented that two actions fulfilled this recommendation: TSA's current program management reviews in which costs are periodically discussed with vendors and the laboratory testing of the ETP's detection capabilities. To fully address this recommendation, a cost-benefit analysis and tests of the ETP's effectiveness to detect explosives in an operational environment are required. As we reported, TSA has not conducted cost-benefit analyses, which, as noted earlier, should compare costs and benefits of alternative solutions. Discussions of maintenance costs with vendors on a periodic basis do not constitute a cost-benefit analysis.

Based on DHS's written comments, we deleted a reference to the 2004 OMB PART review in a footnote because of updated information from OMB's 2008 PART review. DHS also provided us with technical comments, which we considered and incorporated in the report where appropriate. In particular, we clarified the wording of a recommendation which originally stated that TSA should develop quantifiable performance measures to assess the extent to which investments in research, development, and deployment of checkpoint screening technologies have mitigated the risks of a terrorist attack. We altered the wording to state that performance measures should be developed to assess progress towards security goals.

As agreed with your offices, unless you publicly announce the contents of this report, we plan no further distribution for 45 days from the report date. At that time, we will send copies of this report to the Secretary of Homeland Security, the Assistant Secretary of the Transportation Security Administration, and appropriate congressional committees.

If you or your staffs have any questions about this report, please contact me at (202) 512-8777 or LordS@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix III.

A handwritten signature in black ink that reads "Stephen Lord". The signature is written in a cursive style with a large, stylized initial "S".

Stephen M. Lord
Director
Homeland Security and Justice

Appendix I: Objectives, Scope, and Methodology

This report addresses the following questions: (1) To what extent has the Transportation Security Administration (TSA) developed a risk-informed strategy to prioritize investments in the research and development of passenger checkpoint screening technologies? (2) What new passenger checkpoint screening technologies has the Department of Homeland Security (DHS) researched, developed, tested and evaluated, procured, and deployed since its creation, and why did TSA halt the first technology deployment that it initiated—the Explosives Trace Portal (ETP)? (3) To what extent has DHS coordinated the research, development, test and evaluation (RDT&E), procurement, and deployment of passenger checkpoint screening technologies internally and with key stakeholders, such as airport operators and technology vendors?

To determine the extent to which TSA has developed a risk-informed strategy to prioritize investments in the research and development of passenger checkpoint screening technologies, we analyzed program documents, TSA’s August 2008 strategic plan for checkpoint technologies, TSA’s September 2007 report on the development of a strategic plan, technology project plans, and funding. We also compared TSA’s strategic plan and DHS’s responses regarding their efforts to manage their research and development investments, with DHS’s guidance from the National Infrastructure Protection Plan on how to utilize risk management principles to target funding.

To determine the extent to which DHS researched, developed, tested and evaluated, procured, and deployed new checkpoint screening technologies since its creation, and to identify why TSA halted deployment of the ETP, we analyzed TSA’s strategic plan for checkpoint technologies, TSA’s Passenger Screening Program (PSP) documentation, including information on the status of technologies being researched, developed, tested and evaluated, procured, and deployed. Regarding the ETPs, we analyzed the functional requirements for the system, contracts with General Electric and Smiths Detection, and test reports for acceptance tests, regression tests, and operational tests. We also reviewed ETP deployment schedules and documentation on operational availability and mean time between critical failure, and interviewed TSA officials about the reasons that the ETP deployment was halted. We also compared the ETP test approach used by S&T and TSA to the Acquisition Management System (AMS) guidance and knowledge-based acquisition best practices.¹ We also

¹See [GAO-06-257T](#).

interviewed TSA and S&T officials to obtain information on current investments in the research, development, and deployment of checkpoint technologies, and conducted site visits to the Transportation Security Laboratory in Atlantic City, New Jersey, and Tyndall Air Force Base, Florida, to observe testing of new checkpoint technologies. We visited the TSL because that is where S&T tests and evaluates technologies, including checkpoint screening technologies. We visited Tyndall Air Force Base because technologies to detect bottled liquids explosives were being tested there. Additionally, we analyzed TSA's passenger screening standard operating procedures and interviewed various TSA headquarters officials, 29 Federal Security Directors, 1 Deputy Federal Security Director, and 5 Assistant Federal Security Directors for Screening, and visited nine airports where the ETPs had been or were to be deployed or new checkpoint screening technologies were undergoing pilot testing. We chose these officials because they are the senior official at the airport in charge of security and manage TSA's role in deploying new technologies at the airport. We selected these nine locations based on the technologies that had been deployed or were being tested, their geography, size, and proximity to research and development laboratories. Of the nine airports we visited, the ETPs had been or were to be deployed to seven of them, and other new checkpoint screening technologies were undergoing pilot demonstrations or testing at two of them. We visited four airports on the east coast, and three airports on the west coast, and two airports located in the west and southwestern regions of the United States. To determine whether the ETP's requirements had been tested prior to procuring and deploying them, we selected a non-probability sample of 8 out of the 157 total requirements. We selected the 8 requirements because they were related to some of the ETP's key functionality requirements, including operational effectiveness, operational suitability, and passenger throughput.

To determine the extent to which DHS has coordinated and collaborated on the RDT&E, procurement, and deployment of passenger screening technologies internally and with key stakeholders, we analyzed program documents, including an August 2006 memorandum of understanding between TSA and S&T for the management of the Transportation Security Laboratory (TSL). Additionally, we interviewed Department of State officials, TSA and S&T officials, seven checkpoint technology vendors, and

airport operators² and other officials at airports where ETPs were initially deployed. Because we selected nonprobability samples of airports to visit and officials to interview, we cannot generalize the results of what we learned to airports nationwide. However, the information we gathered from these locations and officials provided us with insights and perspectives on DHS's efforts to operationally test and evaluate, and deploy checkpoint technologies that could only be obtained from officials stationed at locations where the technologies had been tested or deployed. We reviewed the Acquisition Management System, the Aviation and Transportation Security Act, the Homeland Security Act of 2002, and the Intelligence Reform and Terrorism Prevention Act and identified requirements and guidance for coordination and collaboration among S&T, TSA, and other stakeholders. We also reviewed S&T's and TSA's coordination activities and compared them to TSA program guidance and GAO's recommended coordination practices regarding agency coordination with external stakeholders.³

We conducted this performance audit from June 2006 through April 2009 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.

²TSA defines an "airport operator" as any persons, who operates an airport serving an aircraft operator or foreign air carrier required to have a security program under 49 C.F.R. parts 1544 or 1546. See 49 C.F.R. § 1540.5.

³GAO, *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, [GAO-06-15](#) (Washington, D.C.: October 21, 2005).

Appendix II: Comments from the Department of Homeland Security

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



**Homeland
Security**

October 6, 2009

Ms. Cathleen A. Berrick
Managing Director, Homeland Security and Justice Team
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Berrick:

Thank you for the opportunity to comment on the draft report: *DHS and TSA Have Researched, Developed, and Begun Deploying Passenger Checkpoint Screening Technologies, but Continue to Face Challenges* (GAO-09-21). The Transportation Security Administration (TSA) appreciates the U.S. Government Accountability Office's (GAO) work in planning, conducting, and issuing this report.

In its report, GAO recommends that TSA improve its analysis of technologies prior to deployment through increased use of risk-management principles and cost-benefit analyses. TSA agrees that there are opportunities for improvement in the deployment of passenger checkpoint technologies and will continue to take steps to advance the testing, deployment, ongoing performance measurement, and stakeholder outreach as each relates to these technologies.

The Passenger Screening Program has embraced the challenge to design and engineer passenger screening as an integrated network of technologies, human factors, and processes to minimize the risk of terrorist attack, using an approach that accounts for the strategic, tactical, and operational realities of the airport environment. As a strategy, the proactive approach builds upon lessons learned from hard intelligence, airport security operations, and TSA organizational experience.

The goals of TSA's security initiatives are to improve explosives detection capability by combining new technology with advanced procedures, establish a cadre of trained behavior detection officers, and incorporate unpredictability into screening measures to thwart terrorist plans. In each operational environment, be it at the checkpoint, in the queues, or in conversations with passengers, TSA created approaches designed to detect and contain risks to minimize catastrophic loss of life or property.

Today, TSA implements passenger checkpoint screening through a risk-informed approach that integrates a variety of sensors, devices, and techniques into a threat detection and response network. This integrated, network-centric approach considers operational requirements to maximize passenger throughput, minimize the number of operating personnel, and protect privacy, all within the constrained footprint of the checkpoint. This

- 2 -

proactive approach relies on an optimized, integrated, mix of networked systems to deter known threats through the passenger screening checkpoint.

TSA's Risk-Informed Strategy

While TSA recognizes that additional risk-informed management initiatives should and will be undertaken, current security technology initiatives have been developed based on an assessment of what TSA believes to be the most cost-effective way of reducing risk across the entire aviation system.

TSA has made resource allocation and technology decisions that were informed by considerations of risk (including threat, vulnerability, and consequence), although not by explicit formal comparative assessment of risk, including threat, vulnerability, and consequence (TVC). This approach was appropriate at TSA's previous level of maturity, and through this process, the Agency gained important insights that have become guiding principles for risk management decisions.

These principles include a deep appreciation for uncertainty and for the limits of what can be known. TSA cannot predict every attack vector in the aviation domain; therefore, our strategy reflects a bias against rigid prioritization and narrow, inflexible solutions that can be overcome by dynamic, adaptive adversaries. TSA continues to focus on developing capabilities that are flexible and adaptable, that cut across risks and threats, and that contain elements of randomness or unpredictability to inject uncertainty into adversaries' planning process. These principles have informed many of TSA's operational and technology decisions in the last few years.

As this work has progressed, TSA has also pursued a formal TVC risk analysis as important decision inputs into future strategy development. TSA has nearly completed a range of formal, comparative, scenario-based TVC risk analyses. The results will be used—along with other factors, such as cost, feasibility, statutory requirements, and privacy—to inform decisions about strategy, operations, and technology development across TSA's aviation security responsibilities, including the Passenger Screening Program (PSP).

At the strategic level, TSA is updating the initial Air Domain Risk Analysis (ADRA), an action item stemming from Homeland Security Presidential Directive 16, with final completion expected in November 2009 and approval expected in the fourth quarter of calendar year 2009. The initial ADRA will compare high-level risks to and through the checkpoint with other high-level risks (*e.g.*, risks involving aviation infrastructure and general aviation) across the domestic U.S. air domain. High-level countermeasures are also evaluated to identify their aggregate, cross-cutting risk-reduction potential across the portfolio of risks. The ADRA will also include a view of risks that originate internationally.

At a more granular level, TSA has been developing the Risk Management and Analysis Toolset (RMAT). RMAT is an agent-based, high-detail simulation model of the commercial aviation security regime, and can be used to model specific risk scenarios (for example, specific types and sizes of explosives) and the risk-reduction potential (across the portfolio of risks) of specific technologies or other countermeasures. The model accounts for dynamic, adaptive adversaries by incorporating intelligence analysis to model the adversary's decision

- 3 -

processes and using that as the threat input, rather than using a direct, static estimation of a threat vector.

This initial set of scenarios is keyed to the actionable decision-support needs of TSA leadership in the near term. The initial RMAT outputs are expected to be available to offer insights to TSA leaders in the second quarter of calendar year 2009. As RMAT data sets and capabilities grow, a larger range of high-detail risks can be modeled; and the effectiveness of a greater range of potential countermeasures can be evaluated.

These improved formal tools for understanding risk in a comprehensive and comparative way—explicitly considering comparative TVC—will offer additional insights and support to TSA leaders making decisions in aviation security, including in the PSP. These tools, and formal risk analysis generally, offer the additional effect of challenging accepted assumptions and surfacing hidden assumptions, providing another benefit to the decision process. Finally, formal comparative TVC risk analyses do not replace, but rather complement and enhance, TSA's principles of risk management described previously. Together they will enable TSA leaders to make decisions on aviation security that are more effective, more flexible, more traceable, and more defensible.

Measuring Performance

TSA conducts a range of threat and vulnerability assessments relative to the checkpoint to select, prioritize, and determine the effectiveness of operational and technology investments. At the field level, Federal Security Directors (FSDs) conduct various types of testing and assessment of operations of their checkpoints. TSA also conducts Joint Vulnerability Assessments (JVAs) in collaboration with the Federal Bureau of Investigation (FBI) at airports on a regular basis. The results of JVAs help provide understanding of common vulnerabilities and trends. On a national level, TSA's Office of Inspection conducts covert testing of checkpoint operations (Red Team testing). This method of measuring the checkpoint's effectiveness, both operationally and technologically, against a simulated attack can identify vulnerabilities that may be specific to one airport or common across the system. Covert tests serve both as a measure of vulnerability that can help inform investment decisions and a reality-based measure of effectiveness of existing operational and technology investments. TSA collaborates with GAO to review Red Team results based on threat injects conducted at checkpoints. In addition, TSA continually monitors field equipment performance data such as Mean Down Time (MDT), Operational Availability (OA), Mean Time to Repair (MTTR), and throughput.

TSA recognized that it needed a more systematic, nationwide framework to assess the effectiveness of the screening process and to identify areas to focus our resources in training and technology. To this end, TSA instituted a comprehensive program to measure screening performance called the Aviation Screening Assessment Program (ASAP). ASAP is aggressively focused on improving recognition of Improvised Explosive Devices (IEDs), and TSA has performed thousands of covert assessments at airports across the country. Through ASAP, we are assessing our performance every day in every aspect of the screening process. Findings from ASAP are reported directly to TSA leadership, who use these performance metrics to make strategic decisions within the screening environment. These decisions include the type of equipment TSA purchases to the type of training TSA delivers to our Transportation Security Officers (TSOs).

- 4 -

In addition, TSA recognizes the value of measuring program progress by developing core program metrics. Through TSA's participation in the Office of Management and Budget (OMB) Program Assessment Rating Tool (PART), the Agency measures both long-term and annual performance metrics. Along with the Reliability, Maintainability, Availability (RMA) metrics, PSP calculates the Operational Availability of Passenger Screening Equipment, the Cost per Bag Screened, and the Ratio of Bags Screened to Passenger Screener Full-Time Equivalent (FTE) Expended. In addition, TSA includes key performance parameters in all technology specifications and tests the technology against those measures. These measures reflect different facets of the purpose of PSP. Contrary to footnote 43 of the draft GAO report, the most recent review (2008) of PSP by OMB through the PART ranked the program as "Effective."

Testing and Evaluation Strategy for New Technologies

TSA is in the process of improving the already robust Testing and Evaluation (T&E) paradigm to ensure that operational effectiveness and suitability of candidate security technology systems are evaluated prior to deployment. Employing the concept of independent and integrated T&E in support of acquisition decisions and other program reviews, this process leverages data from multiple developmental and operational testing sources, accredited vendor data, modeling and simulation, and other special analyses (as required), in accordance with T&E and systems engineering principles and best practices, to streamline T&E requirements while still providing a credible and comprehensive evaluation product. The system-specific integrated T&E strategy addresses technical and operational requirements, considering the contributions of people, processes, and technologies, to provide a single portrait of anticipated mission capabilities for decision makers. TSA is also active in the U.S. Department of Homeland Security (DHS) T&E Council, which will lead to implementation of best practices for T&E across DHS.

TSA has prepared a Test and Evaluation Master Plan (TEMP) for the PSP program and is implementing a formal testing process specified in the TEMP, consistent with DHS's new Acquisition Directive 102. The TEMP establishes a framework that provides an overview of the testing processes followed for all PSP technologies to ensure products meet our specifications, are safe, and operationally effective. The test and evaluation strategy is consistent with the program acquisition strategy. All PSP technology projects follow this testing process, which includes, at a minimum, qualification test and evaluation (QT&E) conducted by the DHS Directorate for Science & Technology (S&T) and operational test and evaluation (OT&E) conducted by TSA. While QT&E tests equipment in a lab setting to validate its operational effectiveness, OT&E tests the product in an airport setting to validate its operational suitability.

Recognizing that Initial Operational Testing and Evaluation (IOT&E) principles mandate examining system detection performance in the field environment, TSA's Office of Security Technology (OST) recently implemented a process to better coordinate realistic threat portrayal with our developmental/technical testing partners. Starting with a common threat baseline, we have developed a process to evaluate system performance (considering operators, systems under test, and concepts of operations) against both active threat agents in a laboratory environment, as well as threat surrogates covertly inserted in the stream of commerce, to better understand the system detection performance envelope. Threat surrogates employed for OT&E purposes have undergone a rigorous verification, validation,

- 5 -

and accreditation (VV&A) process to ensure that stimulants not only generate appropriate threat signatures (and equivalent responses) relative to the technologies of interest, but also can be strongly correlated back to the active threat and appropriate segment of the threat space for the system of interest.

As much of our operational testing is conducted in active environments, in situations where security decisions are being made with systems under test (to most realistically demonstrate operational performance), test design and execution is structured to ensure that test conduct does not degrade the current security posture within the venue. Depending on the specific test, TSA may employ redundant processes and technologies to minimize potential security risks prior to operational test execution. It should also be noted that detection effectiveness, as per TSA testing strategy, is always measured and confirmed in the laboratory setting prior to operational testing in the field.

Transportation Security Integration Facility Testing (TSIF)

TSA has completed the construction of a state-of-the-art facility permitting emerging technologies to be tested for extended periods of time while simulating a variety of operational conditions. This facility will allow TSA to evaluate future maintenance needs and the most efficient operational configurations of new equipment while avoiding disruption to the flow of passengers at checkpoints. The TSIF began operations in January 2009.

Explosives Trace Portal (ETP) Testing and Deployment

In response to a growing concern that terrorists may try to destroy an airplane by packing explosives on their person, TSA tested, procured, and deployed ETP technology from 2004 to 2006. TSA followed its standard technology development process for the ETP, which includes requirements development, testing, procurement, and deployment.

TSA and the DHS S&T followed a formalized testing process, including laboratory and field testing, from April 2004 to January 2006, to validate the effectiveness and suitability of ETPs prior to full-scale deployment. QT&E testing of two vendors' submissions was completed by the Transportation Security Laboratory (TSL) in 2004, confirming the ETP technology was effective in detecting explosives in accordance with TSA's technical detection standards. TSA proceeded with airport operational assessments by fielding five General Electric (GE) ETP systems in 2004. During the field evaluations, TSA assessed the suitability of the system and the Portal Quality Control (PQC) patches, to evaluate the quality of the patches and the application process in a checkpoint environment. As the GAO report noted, the PQC patch performed unfavorably in the February 2005 tests. The test report also indicated that a combination of factors, including the method of testing, environmental conditions, the undetermined shelf life of PQC patches, and the possible variance between levels of explosive materials in the PQC patch, which could have affected detection performance. It is important to note that detection effectiveness was established at the TSL in 2004 and that the PQC assessment demonstrated that the airport assessments did not accurately represent the ETP detection performance, since the reliability of the quality control items was unconfirmed in the field.

The ETPs were further tested by S&T at Idaho National Engineering and Environmental Laboratory (INEEL) in 2005 using methods that were not available to the TSL at that time

- 6 -

(live explosives). The testing at INEEL was presented to TSA by S&T as part of developmental data collection effort for research and development purposes. The INEEL test administrator who conducted the test was not authorized to perform qualification testing on the ETPs, nor was it considered as part of the detection effectiveness assessment. The performance of the ETPs during this testing was not assessed against the established standards.

S&T and TSA proceeded to further assess modified ETP systems from December 2004 to February 2005, reviewing software modifications performed by the vendor. The February 2005 review concluded that the requirements for detection were met by the modified ETP systems. TSA proceeded with another round of airport operational assessments from April to May 2005 to further validate operational suitability. Field test results demonstrated satisfactory performance, indicating the equipment was ready for full-scale deployment. In April 2006, TSA began deploying ETPs to airports.

Additional Testing

In 2006, TSA initiated another round of laboratory testing of the ETP to evaluate its operational effectiveness. During April and May of 2006, INEEL conducted testing on both vendor submissions that revealed deficiencies in reliable performance. Once these test results were received, along with exhibited performance issues with the fielded units, TSA's Office of Acquisitions formally notified the ETP vendor in June 2006 that TSA would not deploy any additional ETPs until the performance issues were addressed. Remaining delivery units were diverted to the TSA warehouse until improvements could be completed and verified. TSA received a reasonable level of assurance from the vendor that these issues could be successfully addressed.

After working with vendors for several months, it was determined that the ETP technology could not be enhanced, and vendors chose not to make additional upgrades. Consequently, TSA did not purchase any further units. TSA determined it was beneficial to keep the existing fielded units in place, since they were effective at detecting explosives when the performance reliability issues did not interfere.

Reliance on New Technologies

As has been described, TSA follows a strict testing process for all technologies before they are fully deployed. It should also be noted that detection ability, as per TSA testing strategy, is always measured and confirmed in the laboratory setting prior to operational testing in the field. For example, in the case of Whole Body Imagers (WBIs), the TSL Independent Test and Evaluation Division (IT&E) has conducted a series of laboratory tests evaluating their performance. The WBI is currently being evaluated against established criteria of threat detection, passenger throughput, and operational availability. In contrast to the ETP, the WBI provides the capability to detect a wider range of threats, including metallic and nonmetallic explosives threats. IT&E has performed five lab assessment-quality test series of WBIs with various devices and/or operational procedures starting in February 2007 and continuing to the present. These tests compare TSO performance while using WBI devices to that of a manual pat-down process. In the event of a WBI alarm, current Standard Operating Procedures (SOPs) require a minimum of a pat-down. All test results indicate the WBI technology is an effective alternative to the pat-down process.

- 7 -

Stakeholder Coordination and Collaboration

TSA appreciates GAO's conclusion that collaboration with S&T; our external stakeholders, including technology vendors; and our airport staff is an essential element to the successful testing, evaluation, and deployment of checkpoint technologies. TSA also values the relationships that have been fostered with industry stakeholders throughout the aviation and security technology communities. While TSA has taken measures to increase coordination with S&T through the development of a Memorandum of Understanding (MOU), the Capstone Integrated Product Team (IPT), and the associated PSP working group, the findings in GAO's report further highlight the need to increase the level of formal coordination with S&T.

TSA has participated in several American Association of Airport Executives conferences. TSA also hosted an airport symposium in the fall of 2007, in which it shared its vision for the future with airport operators and the public. TSA's OST regularly participates in outreach conferences to discuss the technologies available for passenger and baggage screening. To better focus its efforts in this regard, TSA has established a new position on checkpoint stakeholder outreach. In addition, TSA partners with DHS to host technical interchange meetings and industry days where Original Equipment Manufacturers are invited to discuss future requirements for various technologies. These efforts should ultimately reduce costs and development time as vendors work to meet TSA's screening requirements.

TSA also makes every effort to effectively coordinate and collaborate with our airport field staff. During deployment of passenger screening technologies, TSA meets weekly with airports to discuss plans, status, and any issues that arise. TSA has also initiated a TSO focus group in which OST periodically meets with a select group of TSOs to gather their input on new technology and process requirements for passenger screening. As part of TSA's OT&E testing conducted for all equipment, TSA gathers input from airport operators and TSOs to ensure the equipment is functioning effectively in an operational environment. Additional outreach for feedback and input will be implemented for the FSD and their staff as appropriate.

General Conclusion

To protect the security of the traveling public, TSA must be flexible and able to adapt quickly to changes in terrorist tactics. This overarching objective is reflected in every research and development (R&D) and technology deployment decision made by the Agency. TSA will continue to strive toward optimizing technological investments based on thorough R&D analysis and risk-management principles, as well as the collaborative testing and evaluation of new technologies.

Recommendation 1: Conduct a complete risk assessment, including threat, vulnerability, and consequence assessments, which would apply to the PSP.

Concur: TSA concurs and has initiated approaches that identify risks at both the strategic and detailed level. At the strategic level, TSA is updating the initial ADRA. Final completion is expected in November 2009 and approval is expected in fourth quarter of calendar year 2009. At a more detailed level, TSA has been developing the RMAT, an agent-

- 8 -

based, high-detail simulation model that can be used to model specific risk scenarios (for example, specific types and sizes of explosives). The RMAT also can be used to model the risk-reduction potential (across the portfolio of risks) of specific technologies or other countermeasures (for example, a specific piece of equipment deployed in a given percentage of locations). The RMAT tool will be used to generate reports that apply specifically to the passenger screening process and will allow PSP to perform analysis at a level not previously available while not disrupting real world checkpoint operations.

Recommendation 2: Develop cost-benefit analyses to assist in prioritizing investments in new checkpoint screening technologies.

Concur: TSA concurs and is incorporating an approach that combines those risks identified in the RMAT tool with detailed Life Cycle Cost Estimates (LCCEs) to make an informed decision on screening technologies that balances levels of risk (based on current threats) with cost-effective procurement projections of available technologies. In addition, as multiple technologies are implemented and overlapped at the checkpoint, the RMAT scenario can be revisited to model the possible effect of the new systems.

Recommendation 3: Develop quantifiable performance measures to assess the extent to which investments in research, development, and deployment of checkpoint screening technologies achieve performance goals for enhancing security at airport passenger checkpoints.

Concur: TSA understands the importance of developing quantifiable performance measures to ensure that investments support goals and enhance security at the checkpoint. TSA already collects quantifiable performance attributes for all potential acquisitions with regard to metrics, such as detection, false alarm rate, and operational availability. These attributes serve as the baseline against which new technology submissions are evaluated and tested. TSA will work to compare and integrate technology performance measures with those included in the PART and to determine what measures improve checkpoint security when overlapped with multiple systems.

Recommendation 4: After conducting a complete risk assessment and completing cost-benefit analyses and quantifiable performance measures for the PSP, incorporate the results of these efforts into the PSP strategy as determined appropriate.

Concur: TSA concurs and will, upon availability, combine results from the RMAT with LCCEs for possible technology solutions that strike a balance between both risk and efficient use of funding. TSA believes that the RMAT process provides highly valuable insights into capability and risk priorities. However, because of the fundamental uncertainty associated with a dynamic terrorist risk, RMAT and the use of proxy measures cannot be assumed to represent risk reduction measures and will instead be used to provide proxy measures and general “what-if” analysis and risk insight. The projected performance of these technologies will be compared against the long term performance metrics for PSP as established by the most recent PART (2008) in order to ensure linkage between goals and technology implementations.

- 9 -

Recommendation 5: To the extent feasible, ensure that operational tests and evaluations have been successfully completed before deploying checkpoint screening technologies to airport checkpoints.

Concur: TSA has prepared a Test and Evaluation Master Plan (TEMP) for the PSP program and is implementing a formal testing process specified in the TEMP, consistent with DHS's new Acquisition Directive 102. The TEMP establishes a framework for incorporating phased-oriented test and evaluation activities that facilitate the acquisition process. All PSP technology projects follow this testing process, which includes, at a minimum, QT&E conducted by the TSL and OT&E conducted by TSA. OT&E tests the product in an airport setting to validate its operational suitability. TSA has established a robust T&E paradigm to ensure that candidate security technology systems are evaluated for operational effectiveness and suitability prior to deployment.

Recommendation 6: Evaluate whether TSA's passenger screening procedures should be revised to require use of appropriate screening procedures such as pat downs where emerging technologies, including the ETPs and whole body imagers, are currently being used at airports, until it is determined that the machines can meet all of their explosives detection requirements in an operational environment.

Concur: TSA was informed by the TSL that all Atlantic-1 requirements for the ETP were met prior to the pilot testing of machines in the field. The use of the ETP at the checkpoint does not prevent nor prohibit the TSO from exercising judgment and performing additional screening procedures, such as a pat-down, when they feel that it is warranted. In addition, as per current SOP guidance, a pat-down is required for ETP alarm resolution. TSA will complete a review of the explosives trace portals to determine if they are cost-effective and operationally feasible to continue using in airports. For WBI, the TSL IT&E has conducted a series of laboratory tests evaluating the performance of whole body imagers. IT&E performed more than five lab assessment quality test series of WBIs (with various devices and/or operational procedures) starting in February 2007 and continuing to present. These tests have compared TSO performance while using WBI devices to that of a manual pat-down process. Also, in the event of a WBI alarm, current SOPs require a minimum of a pat-down. All results indicate the WBI technology is an effective alternative to the pat-down process.

Recommendation 7: Evaluate all future checkpoint screening technologies prior to testing or using them at airports to determine whether appropriate passenger screening procedures, such as pat downs, should remain in place until the performance of the technologies has been validated through operational test and evaluation.

Concur: TSA will continue to follow its formal test and evaluation process to ensure all checkpoint screening technologies are operationally effective prior to testing or using them in airport settings.


Recommendation 8: Evaluate the benefits, such as the explosives detection effectiveness and deterrent effect, of the ETPs that are being used in airports, and compare the benefits to the costs to operate and maintain this technology to determine whether it is cost-effective to continue to use the machines in airports.

- 10 -

Concur: TSA has already implemented this recommendation through a current and ongoing process of evaluation for the ETP that includes periodic Program Management Reviews (PMRs) with the vendor during which cost-related items are discussed. The detection effectiveness of the ETP has been established in multiple lab tests, but TSA does not feel that deterrence is a measurable quality. TSA has already begun making progress implementing GAO's recommendations. This progress demonstrates our commitment to continual improvement to ensure the security of the traveling public.

Thank you for the opportunity to provide comments to the draft report.

Sincerely yours,



Jerald E. Levine

Director

Departmental GAO/OIG Liaison Office

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Stephen M. Lord, (202) 512-8777 or LordS@gao.gov

Staff Acknowledgments

In addition to the contact named above, Robert Goldenkoff, Acting Director; E. Anne Laffoon and Steve Morris, Assistant Directors; and Joseph E. Dewechter, Analyst-in-Charge, managed this assignment. Carissa Bryant, Chase Cook, Orlando Copeland, Neil Feldman, and Ryan MacMaster made significant contributions to the work. Charles Bausell, Jr., Richard Hung, and Stanley Kostyla assisted with design, methodology, and data analysis. Michele Mackin assisted with acquisition and contracting issues. Sally Williamson, Linda Miller, and Kathryn Godfrey provided assistance in report preparation, and Thomas Lombardi provided legal support.

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 Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to 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 Web site, <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.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

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

Congressional Relations

Ralph Dawn, Managing Director, dawnr@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

