United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Transportation Security and Infrastructure Protection, Committee on Homeland Security, House of Representatives

For Release on Delivery
Expected at 2:00 p.m. EDT
Wednesday, March 17, 2010

AVIATION SECURITY

TSA Is Increasing Procurement and Deployment of the Advanced Imaging Technology, but Challenges to This Effort and Other Areas of Aviation Security Remain

Statement of Steve Lord, Director
Homeland Security and Justice Issues

March 17, 2010

AVIATION SECURITY

TSA Is Increasing Procurement and Deployment of the Advanced Imaging Technology, but Challenges to This Effort and Other Areas of Aviation Security Remain

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-10-484T, a testimony before the Subcommittee on Transportation Security and Infrastructure Protection, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

The attempted bombing of Northwest flight 253 highlighted the importance of detecting improvised explosive devices on passengers. This testimony focuses on (1) the Transportation Security Administration's (TSA) efforts to procure and deploy advanced imaging technology (AIT), and related challenges; and (2) TSA's efforts to strengthen screening procedures and technology in other areas of aviation security, and related challenges. This testimony is based on related products GAO issued from March 2009 through January 2010, selected updates conducted from December 2009 through March 2010 on the AIT procurement, and ongoing work on air cargo security. For the ongoing work and updates, GAO obtained information from the Department of Homeland Security (DHS) and TSA and interviewed senior TSA officials regarding air cargo security and the procurement, deployment, operational testing, and assessment of costs and benefits of the AIT.

What GAO Recommends

GAO is not making new recommendations. In past reports, GAO has recommended, among other things, that TSA operationally test screening technologies prior to deployment and assess costs and benefits of screening technology investments. DHS concurred and is working to address the recommendations. DHS provided comments to this statement, which were incorporated.

View GAO-10-484T or key components.
For more information, contact Steve Lord at (202) 512-4379 or lords@gao.gov.

What GAO Found

In response to the December 25, 2009, attempted attack on Northwest flight 253, TSA revised the AIT procurement and deployment strategy, increasing the planned deployment of AITs from 878 to 1,800 units and using AITs as a primary—instead of a secondary—screening measure where feasible; however, challenges remain. In October 2009, GAO reported on the challenges TSA faced deploying new technologies such as the explosives trace portal (ETP) without fully testing them in an operational environment, and recommended such testing prior to future deployments. TSA officials concurred and stated that, unlike the ETP, operational testing for the AIT was successfully completed late in 2009 before its deployment was fully initiated. While officials said AITs performed as well as physical pat downs in operational tests, it remains unclear whether the AIT would have detected the weapon used in the December 2009 incident based on the preliminary information GAO has received. GAO is verifying that TSA successfully completed operational testing of the AIT. In October 2009, GAO also recommended that TSA complete cost-benefit analyses for new passenger screening technologies. While TSA conducted a life-cycle cost estimate and an alternatives analysis for the AIT, it reported that it has not conducted a cost-benefit analysis of the original deployment strategy or the revised AIT deployment strategy, which proposes a more than twofold increase in the number of machines to be procured. GAO estimates increases in staffing costs alone due to doubling the number of AITs that TSA plans to deploy could add up to $2.4 billion over its expected service life. While GAO recognizes that TSA is attempting to address a vulnerability exposed by the December 2009 attempted attack, a cost-benefit analysis is important as it would help inform TSA's judgment about the optimal deployment strategy for the AITs, and how best to address this vulnerability considering all elements of the screening system.

TSA has also taken actions towards strengthening other areas of aviation security but continues to face challenges. For example, TSA has taken steps to meet the statutory mandate to screen 100 percent of air cargo transported on passenger aircraft by August 2010, including developing a program to share screening responsibilities across the air cargo supply chain. However, as GAO reported in March 2009, a number of challenges to this effort exist, including attracting participants to the TSA screening program, completing technology assessments, and overseeing additional entities that it expects to participate in the program. GAO is exploring these issues as part of an ongoing review of TSA's air cargo security program which GAO plans to issue later this year. Further, while TSA has taken a variety of actions to strengthen the security of commercial airports, GAO reported in September 2009 that TSA continues to face challenges in several areas, such as assessing risk and evaluating worker screening methods. In September 2009, GAO also recommended that TSA develop a national strategy to guide stakeholder efforts to strengthen airport perimeter and access control security, to which DHS concurred.

Madame Chairwoman and Members of the Subcommittee,

I am pleased to be here today to discuss the Transportation Security Administration's (TSA) progress in securing passenger checkpoints and other areas of commercial aviation. In response to the December 25, 2009, attempted bombing of Northwest flight 253, the Secretary of Homeland Security announced five corrective actions to improve aviation security, including accelerating deployment of the advanced imaging technology (AIT)—formerly called the Whole Body Imager—to identify materials such as those used in the attempted Christmas Day bombing. The AITs produce an image of a passenger's body that TSA personnel use to look for anomalies, such as explosives. TSA is deploying AITs to airport passenger checkpoints to enhance its ability to detect explosive devices and other prohibited items on passengers. Passengers undergo either primary or secondary screening at these checkpoints. Primary screening is conducted on all airline passengers before they enter the sterile area of an airport and involves passengers walking through a metal detector and their carry-on items being subjected to X-ray screening.[1] Secondary screening is conducted on selected passengers and involves additional screening of both passengers and their carry-on items. While screening passengers at the checkpoint is a vital layer of security, it is also important to ensure the security of other areas of commercial aviation, such as air cargo transported on passenger aircraft, and airport worker screening and checked baggage screening.

TSA's passenger checkpoint screening system comprises three elements: (1) personnel responsible for, among other things, screening passengers and baggage; (2) the policies and procedures that govern the different aviation security programs; and (3) the technology used to screen passengers and baggage. All three elements—people, process, and technology—collectively help determine the effectiveness and efficiency of passenger checkpoint screening, and our past work in this area has

[1]Sterile areas are areas of airports where passengers wait after screening to board departing aircraft.

addressed all three elements of the system.[2] Similarly, securing the flying public involves tradeoffs between security, privacy, and the efficient flow of commerce. Striking the right balance between these three goals is an ongoing challenge facing TSA.

My testimony today focuses on (1) TSA's plans to procure, deploy, and test AITs to enhance the security of the passenger checkpoint, and any challenges TSA faces in this effort; and (2) TSA's efforts to strengthen screening procedures and technology in other areas of aviation security, and any related challenges the agency faces in these areas.

This statement is based on related GAO reports and testimonies we issued from March 2009 through January 2010, as well as preliminary observations based on ongoing work—from October 2008 through February 2010—to be completed later this year assessing the progress that DHS and its component agencies have made in addressing challenges related to air cargo security.[3] To conduct all of this work, we reviewed relevant documents related to the programs reviewed, and interviewed cognizant Department of Homeland Security (DHS) and TSA officials. All of this work was conducted in accordance with generally accepted government auditing standards, and our previously published reports contain additional details on the scope and methodology for those reviews. In addition, this statement contains selected updates conducted from December 2009 through March 2010 on TSA's effort to procure and deploy the AIT. For the updates, we obtained information from DHS and

[2]See for example, GAO, *Homeland Security: Better Use of Terrorist Watchlist Information and Improvements in Deployment of Passenger Screening Checkpoint Technologies Could Further Strengthen Security*, GAO-10-401T (Washington, D.C.: Jan. 27, 2010); *Aviation Security: DHS and TSA Have Researched, Developed, and Begun Deploying Passenger Checkpoint Screening Technologies, but Continue to Face Challenges*, GAO-10-128 (Washington, D.C.: Oct. 7, 2009); *Homeland Security: DHS's Progress and Challenges in Key Areas of Maritime, Aviation, and Cybersecurity*, GAO-10-106 (Washington, D.C.: Dec. 2, 2009); *Aviation Security: TSA Has Completed Key Activities Associated with Implementing Secure Flight, but Additional Actions Are Needed to Mitigate Risks*, GAO-09-292 (Washington, D.C.: May 13, 2009); *Aviation Security: Preliminary Observations on TSA's Progress and Challenges in Meeting the Statutory Mandate for Screening Air Cargo on Passenger Aircraft*, GAO-09-422T (Washington, D.C.: Mar. 18, 2009); *Aviation Security: Vulnerabilities Exposed Through Covert Testing of TSA's Passenger Screening Process*, GAO-08-48T (Washington, D.C.: Nov. 15, 2007); and *Terrorist Watch List Screening: Opportunities Exist to Enhance Management Oversight, Reduce Vulnerabilities in Agency Screening Processes, and Expand Use of the List*, GAO-08-110 (Washington, D.C.: Oct. 11, 2007).

[3]GAO-10-401T; GAO-10-128; GAO-10-106, and GAO-09-422T.

TSA on the AIT and interviewed senior TSA officials regarding the planned procurement, deployment, operational testing and evaluation, and assessment of benefits and costs of the AITs. We conducted these updates 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 based on our audit objectives.

Background

Airline Passenger Screening Using Checkpoint Technology

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 carrying of any unauthorized explosive, incendiary, weapon, or other prohibited item on board an aircraft or into a sterile area. Screeners inspect individuals for prohibited items at designated screening locations. TSA developed standard operating procedures for screening passengers at airport checkpoints. Primary screening is conducted on all airline passengers before they enter 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, as well as passengers whose carry-on items have been identified by the X-ray machine as potentially containing prohibited items. Secondary screening involves additional means for screening passengers, such as by hand wand; physical pat down; or other screening methods such as the AIT.

Role of DHS Science & Technology Directorate

Within DHS, both 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 and provides input to S&T during the research and development of new technologies, which TSA then procures and deploys. Because S&T and TSA share responsibilities related to the research, development, test and evaluation (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.

Air Cargo Security

Air cargo can be shipped in various forms, including unit load devices (ULD) that allow many packages to be consolidated into one container or pallet; wooden crates; or individually wrapped/boxed pieces, known as loose or break-bulk cargo. Participants in the air cargo shipping process include shippers, such as manufacturers; freight forwarders, who consolidate cargo from shippers and take it to air carriers for transport; air cargo handling agents, who process and load cargo onto aircraft on behalf of air carriers; and air carriers that load and transport cargo.[4] TSA's responsibilities include, among other things, establishing security requirements governing domestic and foreign passenger air carriers that transport cargo and domestic freight forwarders.

Airport Perimeter Security and Access Control

Airport perimeter and access control security is intended to prevent unauthorized access into secured airport areas, either from outside the airport complex or from within. Airport operators generally have direct day-to-day responsibility for maintaining and improving perimeter and access control security, as well as implementing measures to reduce worker risk. However, TSA has primary responsibility for establishing and implementing measures to improve security operations at U.S. commercial airports—that is, TSA-regulated airports—including overseeing airport operator efforts to maintain perimeter and access control security.[5] Airport workers may access sterile areas through TSA security checkpoints or through other access points that are secured by the airport operator. The airport operator is also responsible, in accordance with its security program, for securing access to secured airport areas where passengers are not permitted. Airport methods used to control access vary, but all access controls must meet minimum performance standards in accordance with TSA requirements.

[4]For purposes of this statement, the term freight forwarders only includes those freight forwarders that are regulated by TSA, also referred to as indirect air carriers.

[5]See generally Aviation and Transportation Security Act, Pub. L. No. 107-71, 115 Stat. 597 (2001).

Increased Deployment of AIT Highlights the Importance of Operational Testing and Cost-Benefit Analysis Prior to Deployment

TSA Plans to Procure and Deploy 1,800 AITs by 2014 and Use Them as a Primary Screening Measure

In response to the December 2009 attempted terrorist attack, TSA has revised its procurement and deployment strategy for the AIT, increasing the number of AITs it plans to procure and deploy. In contrast with its prior strategy, the agency now plans to acquire and deploy 1,800 AITs (instead of the 878 units it had previously planned to acquire) and to use them as a primary screening measure where feasible rather than solely as a secondary screening measure. According to a senior TSA official, the agency is taking these actions in response to the Christmas Day 2009 terrorist incident. These officials stated that they anticipate the AIT will provide enhanced security benefits compared to walk-through metal detectors, such as enhanced detection capabilities for identifying nonmetallic threat objects and liquids. TSA officials also stated that the AIT offers greater efficiencies because it allows TSA to more rigorously screen a greater number of passengers in a shorter amount of time while providing a detection capability equivalent to a pat down. For example, the AIT requires about 20 seconds to produce and interpret a passenger's image as compared with 2 minutes required for a physical pat down. A senior official also stated that TSA intends to continue to offer an alternative but comparable screening method, such as a physical pat down, for passengers who prefer not to be screened using the AIT.

The AIT produces an image of a passenger's body that a screener interprets. The image identifies objects, or anomalies, on the outside of the physical body but does not reveal items beneath the surface of the skin, such as implants. TSA plans to procure two types of AIT units: one type uses millimeter-wave and the other type uses backscatter X-ray technology. Millimeter-wave technology beams millimeter-wave radio-frequency energy over the body's surface at high speed from two antennas simultaneously as they rotate around the body. The energy reflected back from the body or other objects on the body is used to construct a three-

dimensional image. Millimeter wave technology produces an image that resembles a fuzzy photo negative. Backscatter X-ray technology uses a low-level X-ray to create a two-sided image of the person. Backscatter technology produces an image that resembles a chalk etching.

As of February 24, 2010, according to a senior TSA official, the agency has deployed 40 of the millimeter-wave AITs and procured 150 backscatter X-ray units in fiscal year 2009. In early March 2010, TSA initiated the deployment of these backscatter units starting with two airports, Logan International Airport in Boston, Massachusetts, and Chicago O'Hare International Airport in Des Plaines, Illinois. TSA officials stated that they do not expect these units to be fully operational, however, until the second or third week of March due to time needed to hire and train additional personnel. TSA estimates that the remaining backscatter X-ray units will be installed at airports by the end of calendar year 2010. In addition, TSA plans to procure an additional 300 AIT units in fiscal year 2010, some of which it plans to purchase with funds from the American Recovery and Reinvestment Act of 2009. In fiscal year 2011, TSA plans to procure 503 AIT units. TSA projects that a total of about 1,000 AIT systems will be deployed to airports by the end of December 2011. In fiscal year 2014 TSA plans to reach full operating capacity, having procured a total of 1,800 units and deployed them to 60 percent of the checkpoint lanes at Category X, I, and II airports.[6] The current projected full operating capacity of 1,800 machines represents a more than two-fold increase from 878 units that TSA had previously planned. TSA officials stated that the cost of the AIT is about $170,000 per unit, excluding training, installation, and maintenance costs. In addition, in the fiscal year 2011 President's budget submission, TSA has requested $218.9 million for 3,550 additional full-time equivalents (FTE) to help staff the AITs deployed in that time frame. From 2012 through 2014, as TSA deploys additional units to reach full operating capacity, additional staff will be needed to operate these units; such staffing costs will recur on an annual basis. TSA officials told us that three FTEs are needed to operate each unit.

Because the AIT presents a full body image of a person during the screening process, concerns have been expressed that the image is an

[6]There are about 450 commercial airports in the United States. TSA classifies airports into one of five categories (X, I, II, III, and IV) based on various factors, such as the total number of takeoffs and landings annually, the extent to which passengers are screened at the airport, and other special security considerations. In general, category X airports have the largest number of passenger boardings, and category IV airports have the smallest.

invasion of privacy. According to TSA, to protect passenger privacy and ensure anonymity, strict privacy safeguards are built into the procedures for use of the AIT. For example, the officer who assists the passenger does not see the image that the technology produces, and the officer who views the image is remotely located in a secure resolution room and does not see the passenger. Officers evaluating images are not permitted to take cameras, cell phones, or photo-enabled devices into the resolution room. To further protect passengers' privacy, ways have been introduced to blur the passengers' images. The millimeter-wave technology blurs all facial features, and the backscatter X-ray technology has an algorithm applied to the entire image to protect privacy. Further, TSA has stated that the AIT's capability to store, print, transmit, or save the image will be disabled at the factory before the machines are delivered to airports, and each image is automatically deleted from the system after it is cleared by the remotely located security officer. Once the remotely located officer determines that threat items are not present, that officer communicates wirelessly to the officer assisting the passenger. The passenger may then continue through the security process. Potential threat items are resolved through a directed physical pat down before the passenger is cleared to enter the sterile area.[7] In addition to privacy concerns, the AITs are large machines, and adding them to the checkpoint areas will require additional space, especially since the operators are physically segregated from the checkpoint to help ensure passenger privacy. Adding a significant number of additional AITs to the existing airport infrastructure could impose additional challenges on airport operators.

[7]TSA stated that it continues to evaluate possible display options that include a "stick figure" or "cartoon-like" form to provide greater privacy protection to the individual being screened while still allowing the unit operator or automated detection algorithms to detect possible threats. DHS is working directly with technology providers to develop advanced screening algorithms for the AIT that would utilize Automatic Target Recognition to identify and highlight possible threats.

TSA Recently Reported Efforts to Strengthen Its Operational Test and Evaluation Process, but It Is Not Clear Whether TSA Has Fully Evaluated the Relative Security Benefits and Costs of the AIT

In October 2009, we reported that TSA had relied on a screening technology in day-to-day airport operations that had not been proven to meet its functional requirements through operational testing and evaluation, contrary to TSA's acquisition guidance and a knowledge-based acquisition approach.[8] We also reported that TSA had not operationally tested the AITs at the time of our review, and we recommended that TSA operationally test and evaluate technologies prior to deploying them.[9] In commenting on our report, TSA agreed with this recommendation. Although TSA does not yet have a written policy requiring operational testing prior to deployment, a senior TSA official stated that TSA has made efforts to strengthen its operational test and evaluation process and that TSA is now complying with DHS's current acquisition directive that requires operational testing and evaluation be completed prior to deployment.[10] According to officials, TSA is now requiring that AIT are to successfully complete both laboratory tests and operational tests prior to deployment.

As we previously reported, TSA's experience with the explosives trace portal (ETP), or "puffers," demonstrates the importance of testing and evaluation in an operational environment.[11] The ETP 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. TSA procured 207 ETPs and in 2006 deployed 101 ETPs to 36 airports, the first deployment of a checkpoint technology initiated by the agency.[12] TSA deployed the ETPs even though tests conducted during 2004 and 2005 on earlier ETP models suggested that they did not demonstrate

[8]GAO-10-128.

[9]Operational testing refers to testing in an operational environment in order to verify that new systems are operationally effective, supportable, and suitable.

[10]DHS Acquisition Management Directive 102-01, Jan. 20, 2010.

[11]We have previously reported that deploying technologies that have not successfully completed operational testing and evaluation can lead to cost overruns and underperformance. 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. 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. See GAO-10-128 and GAO, *Best Practices: Using a Knowledge-Based Approach to Improve Weapon Acquisition*, GAO-04-386SP (Washington, D.C.: Jan. 2004).

[12]TSA deployed the ETPs from January to June 2006.

reliable performance. Furthermore, the ETP models that were subsequently deployed were not tested to prove their effective performance in an operational environment, contrary to TSA's acquisition guidance, which recommends such testing. As a result, TSA procured and deployed ETPs without assurance that they would perform as intended in an operational environment. TSA officials stated that they deployed the machines without resolving these issues to respond quickly to the threat of suicide bombers. In June 2006 TSA halted further deployment of the ETP because of performance, maintenance, and installation issues. According to a senior TSA official, as of December 31, 2009, all but 9 ETPs have been withdrawn from airports, and 18 ETPs remain in inventory.

Following the completion of our review, TSA officials told us that the AIT successfully completed operational testing at the end of calendar year 2009 before its deployment was fully initiated. The official also stated that the AIT test results were provided and reviewed by DHS's Acquisition Review Board prior to the board approving the AIT deployment. According to TSA's threat assessment, terrorists have various techniques for concealing explosives on their persons, as was evident in Mr. Abdulmutallab's attempted attack on December 25, when he concealed an explosive in his underwear. While TSA officials stated that the laboratory and operational testing of the AIT included placing explosive material in different locations on the body,[13] it remains unclear whether the AIT would have been able to detect the weapon Mr. Abdulmutallab used in his attempted attack based on the preliminary TSA information we have received. We are in the process of reviewing these operational tests to assess the AIT's detection capabilities and to verify that TSA successfully completed operational testing of the AIT.

In addition, while TSA officials stated that the AITs performed as well as physical pat downs in operational testing, TSA officials also reported they have not conducted a cost-benefit analysis of the original or revised AIT deployment strategy. We reported in October 2009 that TSA had not conducted a cost-benefit analysis of checkpoint technologies being researched and developed, procured, and deployed and recommended that it do so. DHS concurred with our recommendation. Cost-benefit analyses are important because they help decision makers determine which protective measures, for instance, investments in technologies or in other security programs, will provide the greatest mitigation of risk for the

[13]The results of TSA's laboratory and operational testing are classified.

resources that are available. TSA officials stated that a cost-benefit analysis was not completed for the AIT because one is not required under DHS acquisition guidance. However, these officials reported that they had completed, earlier in the program, a life-cycle cost estimate and an analysis of alternatives for the AIT as required by DHS, which, according to agency officials, provides equivalent information to a cost-benefit analysis. We are in the process of reviewing the alternatives analysis that was completed in 2008 and life-cycle cost estimates which TSA provided to us on March 12, 2010, to determine the extent to which these estimates reflect the additional costs to staff these units. We estimate that, based on TSA's fiscal year 2011 budget request and current AIT deployment strategy, increases in staffing costs due to doubling the number of AITs that TSA plans to deploy could add up to $2.4 billion over the expected service life of this investment.[14]

While we recognize that TSA is taking action to address a vulnerability of the passenger checkpoint exposed by the December 25, 2009, attempted attack, we continue to believe that, given TSA's expanded deployment strategy, conducting a cost-benefit analysis of TSA's AIT deployment is important. An updated cost-benefit analysis would help inform TSA's judgment about the optimal deployment strategy for the AITs, as well as provide information to inform the best path forward, considering all elements of the screening system, for addressing the vulnerability identified by this attempted terrorist attack.

[14]To estimate the cost of the additional staff needed to operate the AIT machines during their service life as a result of TSA's increased deployment of the AIT, we used information in the President's Budget Request for Fiscal Year 2011 and from interviews with TSA officials. We identified staffing costs to operate each AIT ($369,764) and multiplied this figure by the number of additional AITs that TSA has recently planned to deploy by 2014 (922 units) to calculate the additional staffing costs, which equaled $340,922,408. We then multiplied the additional staffing costs of $340,922,408 by 7 years to calculate the additional staffing cost to operate additional AIT units during their expected service life, which equaled $2,386,456,856.

TSA Has Made Progress in Securing Air Cargo and Airport Access, but Challenges Remain

TSA Has Made Progress in Meeting the Air Cargo Screening Mandate, but Faces Participation, Technology, Oversight, and Inbound-Cargo Challenges

As we previously reported in March 2009, based on preliminary observations from ongoing work, TSA has taken several key steps to meet the statutory mandate to screen 100 percent of air cargo transported on passenger aircraft by August 2010.[15] Among the steps that TSA has taken to address domestic air cargo screening, the agency has revised its security programs to require more cargo to be screened; created the Certified Cargo Screening Program (CCSP), a voluntary program to allow screening to take place earlier in the shipping process and at various points in the air cargo supply chain—including before the cargo is consolidated; issued an interim final rule, effective November 16, 2009, that, among other things, codifies the statutory air cargo screening requirements of the 9/11 Commission Act and establishes requirements for entities participating in the CCSP;[16] established a technology pilot program to operationally test explosives trace detection (ETD) and X-ray technology;[17] and expanded its explosives detection canine program.

[15]GAO-09-422T. The Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act) requires that by August 2010, 100 percent of cargo—domestic and inbound—transported on passenger aircraft be physically screened. The 9/11 Commission Act establishes minimum standards for screening air cargo and defines screening for purposes of the air cargo screening mandate as a physical examination or nonintrusive methods of assessing whether cargo poses a threat to transportation security. Solely performing a review of information about the contents of cargo or verifying the identity of the cargo's shipper does not constitute screening for purposes of satisfying the mandate. See Pub. L. No. 110-53, § 1602(a), 121 Stat. 266, 477-79 (codified at 49 U.S.C. § 44901(g)). For the purposes of this statement, domestic air cargo refers to cargo transported by air within the United States and from the United States to a foreign location by both U.S. and foreign-based air carriers; and inbound cargo refers to cargo transported by U.S. and foreign-based air carriers from a foreign location to the United States.

[16]See Air Cargo Screening, 74 Fed. Reg. 47672 (Sept. 16, 2009).

[17]ETD requires human operators to collect samples of items to be screened with swabs, which are chemically analyzed to identify any traces of explosives material.

While these steps are encouraging, TSA faces several challenges in meeting the air cargo screening mandate. First, although industry participation in the CCSP is vital to TSA's approach to move screening responsibilities across the U.S. supply chain, the voluntary nature of the program may make it difficult to attract program participants needed to screen the required levels of domestic cargo. Second, while TSA has taken steps to test technologies for screening and securing air cargo, it has not yet completed assessments of the various technologies it plans to allow air carriers and program participants to use in meeting the August 2010 screening mandate. According to TSA officials, several X-ray and explosives detection systems (EDS) technologies successfully passed laboratory testing, and TSA placed them on a December 2009 list of qualified products that industry can use to screen cargo after August 2010.[18] TSA plans to conduct field testing and evaluation of these technologies in an operational environment. In addition, TSA plans to begin laboratory testing for ETD, Electronic Metal Detection (EMD), and additional X-ray technologies in early 2010, and anticipates including these technologies on the list of qualified products the industry can use by the summer of 2010, before proceeding with operational testing.[19] As we previously reported, based on preliminary observations from ongoing work, X-ray and ETD technologies, which have not yet been fully tested for effectiveness, are currently being used by industry participants to meet air cargo screening requirements.[20] We are examining this issue in more detail as part of our ongoing review of TSA's air cargo security efforts, to be issued later this year.

Third, TSA faces challenges overseeing compliance with the CCSP due to the size of its current Transportation Security Inspector (TSI) workforce. Under the CCSP, in addition to performing inspections of air carriers and freight forwarders, TSIs are to also perform compliance inspections of new regulated entities that voluntarily become certified cargo screening facilities (CCSF), as well as conduct additional CCSF inspections of existing freight forwarders. TSA officials have stated that the agency is evaluating the required number of TSIs to fully implement and oversee the program. Completing its staffing study may help TSA determine whether it

[18]EDS uses computer-aided tomography X-rays to examine objects inside baggage and identify the characteristic signatures of threat explosives.

[19]EMD devices are capable of detecting metallic-based explosives, such as wires, within a variety of perishable commodities at the cargo-piece, parcel, and pallet level.

[20]GAO-09-422T.

has the necessary staffing resources to ensure that entities involved in the CCSP are meeting TSA requirements to screen and secure air cargo.[21] As part of our ongoing work, we are exploring to what extent TSA is undertaking a staffing study.

Finally, TSA has taken some steps to meet the screening mandate as it applies to inbound cargo but does not expect to achieve 100 percent screening of inbound cargo by the August 2010 deadline. TSA revised its requirements to, in general, require carriers to screen 50 percent of nonexempt inbound cargo. TSA also began harmonization of security standards with other nations through bilateral and quadrilateral discussions.[22] In addition, TSA continues to work with Customs and Border Protection (CBP) to leverage an existing CBP system to identify and target high-risk air cargo. However, TSA does not expect to meet the mandated 100 percent screening level by August 2010. This is due, in part, to challenges TSA faces in harmonizing the agency's air cargo security standards with those of other nations. Moreover, TSA's international inspection resources are limited. We will continue to explore these issues as part of our ongoing review of TSA's air cargo security efforts, to be issued later this year.

[21]For additional information on TSA's staffing study, see GAO, *Aviation Security: Status of Transportation Security Inspector Workforce*, GAO-09-123R (Washington D.C.: Feb. 6, 2009).

[22]The term harmonization is used to describe countries' efforts to coordinate their security practices to enhance security and increase efficiency by avoiding duplication of effort.

TSA Has Taken Actions to Strengthen Airport Security, but Faces Challenges That Include Assessing Risk and Evaluating Worker Screening Methods

In our September 2009 report on airport security, we reported that TSA has implemented a variety of programs and protective actions to strengthen the security of commercial airports.[23] For example, in March 2007, TSA implemented a random worker screening program—the Aviation Direct Access Screening Program (ADASP)—nationwide to enforce access procedures, such as ensuring that workers do not possess unauthorized items when entering secured areas.[24] In addition, TSA has expanded requirements for background checks and for the population of individuals who are subject to these checks, and has established a statutorily directed pilot program to assess airport security technology.[25]

As we reported in September 2009, while TSA has taken numerous steps to enhance airport security, it continues to face challenges in several areas, such as assessing risk, evaluating worker screening methods, addressing airport technology needs, and developing a unified national strategy for airport security.[26] For example, while TSA has taken steps to assess risk related to airport security, it has not conducted a comprehensive risk assessment based on assessments of threats, vulnerabilities, and consequences, as required by DHS's National Infrastructure Protection Plan. To address these issues, we recommended, among other things, that TSA develop a comprehensive risk assessment of airport security and milestones for its completion, and evaluate whether the current approach to conducting vulnerability assessments appropriately assesses vulnerabilities. DHS concurred with these recommendations and stated that TSA is taking actions to implement them.

Our September 2009 report also reported the results of TSA efforts to help identify the potential costs and benefits of 100 percent worker screening

[23]GAO, *Aviation Security: A National Strategy and Other Actions Would Strengthen TSA's Efforts to Secure Commercial Airport Perimeters and Access Controls*, GAO-09-399 (Washington, D.C.: Sept. 30, 2009).

[24]For the purposes of this statement "secured area" is used generally to refer to areas specified in an airport security program that require restricted access. See 49 C.F.R. §§ 1540.5, 1542.201.

[25]According to TSA officials, the agency established this program in response to a provision enacted through the Aviation and Transportation Security Act. See Pub. L. No. 107-71 § 106(d), 115 Stat. at 610 (codified at 49 U.S.C. § 44903(c)(3)).

[26]GAO-09-399.

and other worker screening methods.[27] In July 2009 TSA issued a final report on the results and concluded that random screening is a more cost-effective approach because it appears "roughly" as effective in identifying contraband items at less cost than 100 percent worker screening.[28] However, the report also identified limitations in the design and evaluation of the program and in the estimation of costs, such as the limited number of participating airports, the limited evaluation of certain screening techniques, the approximate nature of the cost estimates, and the limited amount of information available regarding operational effects and other costs. Given the significance of these limitations, we reported in September 2009 that it is unclear whether random worker screening is more or less cost effective than 100 percent worker screening. In addition, TSA did not document key aspects of the pilot's design, methodology, and evaluation, such as a data analysis plan, limiting the usefulness of these efforts. To address this, we recommended that TSA ensure that future airport security pilot program evaluation efforts include a well-developed and well-documented evaluation plan, to which DHS concurred.

Moreover, although TSA has taken steps to develop biometric worker credentialing, it is unclear to what extent TSA plans to address statutory requirements regarding biometric technology, such as developing or requiring biometric access controls at airports, establishing comprehensive standards, and determining the best way to incorporate these decisions into airports' existing systems.[29] To address this issue, we have recommended that TSA develop milestones for meeting statutory requirements for, among other things, performance standards for biometric airport access control systems. DHS concurred with this recommendation. Finally, TSA's efforts to enhance the security of the

[27]To respond to the threat posed by airport workers, the Explanatory Statement accompanying the DHS Appropriations Act, 2008, directed TSA to use $15 million of its appropriation to conduct a pilot program at seven airports. Explanatory Statement accompanying Division E of the Consolidated Appropriations Act, 2008, Pub. L. No. 110-161, Div. E, 121 Stat. 1844, 2042 (2007), at 1048. While the Statement refers to these pilot programs as airport employee screening pilots, for the purposes of this statement, we use "worker screening" to refer to the screening of all individuals who work at the airport.

[28]Transportation Security Administration, *Airport Employee Screening Pilot Program Study: Fiscal Year 2008 Report to Congress* (Washington, D.C., July 7, 2009).

[29]Among other things, the Intelligence Reform and Terrorism Prevention Act of 2004 directed TSA, in consultation with industry representatives, to establish comprehensive technical and operational system requirements and performance standards for the use of biometric identifier technology in airport access control systems. See Pub. L. No. 108-458, § 4011, 118 Stat. 3638, 3712-14 (2004) (codified at 49 U.S.C. § 44903(h)(5)).

nation's airports have not been guided by a national strategy that identifies key elements, such as goals, priorities, performance measures, and required resources. To better ensure that airport stakeholders take a unified approach to airport security, we recommended that TSA develop a national strategy that incorporates key characteristics of effective security strategies, such as measurable goals and priorities, to which DHS concurred and stated that TSA is taking action to implement it.

Project Newton May Result in New Explosives Testing Standards for TSA's Screening Technology

As we discussed in our October 2009 report, TSA and the DHS Science and Technology Directorate (S&T) are pursuing an effort—known as Project Newton—which uses computer modeling to determine the effects of explosives on aircraft and develop new requirements to respond to emerging threats from explosives.[30] 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. 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, the Federal Aviation Administration, 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 placed in different locations within various aircraft models. As discussed in our October 2009 report, TSA and S&T officials expect that

[30] GAO-10-128.

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. We are currently reviewing Project Newton and will report on it at a later date.

Madame Chairwoman, that concludes my statement and I would be happy to answer any questions.

Contacts and Acknowledgements

For additional information about this statement, please contact Stephen M. Lord at (202) 512-4379 or lords@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement.

In addition to the contact named above, staff who made key contributions to this statement were E. Anne Laffoon and Steve D. Morris, Assistant Directors; Nabajyoti Barkakati, Carissa Bryant, Frances Cook, Joseph E. Dewechter, Amy Frazier, Barbara Guffy, David K. Hooper, Richard B. Hung, Lori Kmetz, Linda S. Miller, Timothy M. Persons, Yanina Golburt Samuels, Emily Suarez-Harris, and Rebecca Kuhlmann Taylor.

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