United States Government Accountability Office

GAO

Testimony
Before the Subcommittee on National Security, Homeland Defense, and Foreign Operations, Committee on Oversight and Government Reform, House of Representatives

For Release on Delivery
Expected at 9:30 a.m. EDT
Wednesday, July 13, 2011

AVIATION SECURITY

TSA Has Taken Actions to Improve Security, but Additional Efforts Remain

Statement of Stephen M. Lord, Director
Homeland Security and Justice Issues

July 13, 2011

AVIATION SECURITY

TSA Has Taken Actions to Improve Security, but Additional Efforts Remain

GAO Accountability * Integrity * Reliability

Highlights

Highlights of GAO-11-807T, a testimony before the Subcommittee on National Security, Homeland Defense, and Foreign Operations, Committee on Oversight and Government Reform, House of Representatives

Why GAO Did This Study

The attempted bombing of Northwest flight 253 in December 2009 underscores the need for effective aviation security programs. Aviation security remains a daunting challenge with hundreds of airports, thousands of aircraft, and thousands of flights daily carrying millions of passengers and pieces of checked baggage. The Department of Homeland Security's (DHS) Transportation Security Administration (TSA) has spent billions of dollars and implemented a wide range of aviation security initiatives. Three key layers of aviation security are (1) TSA's Screening of Passengers by Observation Techniques (SPOT) program designed to identify persons who may pose a security risk; (2) airport perimeter and access controls security; and (3) checked baggage screening systems. This testimony provides information on the extent to which TSA has taken actions to validate the scientific basis of SPOT, strengthen airport perimeter security and access controls, and deploy more effective checked baggage screening systems. This statement is based on prior reports GAO issued from September 2009 through July 2011 and selected updates in June and July 2011. GAO analyzed documents on TSA's progress in strengthening aviation security, among other things.

What GAO Recommends

GAO has made recommendations in prior work to strengthen TSA's SPOT program, airport security efforts, checked baggage screening efforts. DHS and TSA generally concurred with the recommendations and have actions under way to address them.

View GAO-11-807T or key components. For more information, contact Stephen M. Lord at (202) 512-8777 or lords@gao.gov.

What GAO Found

DHS has completed an initial study to validate the scientific basis of the SPOT program; however, additional work remains to fully validate the program. GAO reported in May 2010 that TSA deployed this program, which uses behavior observation and analysis techniques to identify potentially high-risk passengers, before determining whether there was a scientifically valid basis for using behavior and appearance indicators as a means for reliably identifying passengers who may pose a risk to the U.S. aviation system. TSA officials said that SPOT was deployed in response to potential threats, such as suicide bombers, and was based on scientific research available at the time. GAO recommended in May 2010 that DHS, as part of its study, assess the methodology to help ensure the validity of the SPOT program. DHS concurred and its April 2011 validation study found that SPOT was more effective than random screening to varying degrees. For example, the study found that SPOT was more effective than random screening at identifying individuals who possessed fraudulent documents and individuals who were subsequently arrested. However, DHS's study was not designed to fully validate whether behavior detection can be used to reliably identify individuals in an airport environment who pose a security risk. The study noted that additional work is needed to comprehensively validate the program. TSA officials are assessing the actions needed to address the study's recommendations.

In September 2009, GAO reported that since 2004 TSA has taken actions to strengthen airport perimeter and access controls security by, among other things, deploying a random worker screening program; however, TSA has not conducted a comprehensive risk assessment or developed a national strategy. Specifically, TSA had not conducted vulnerability assessments for 87 percent of the approximately 450 U.S. airports regulated by TSA at that time. GAO recommended that TSA develop (1) a comprehensive risk assessment and evaluate the need to assess airport vulnerabilities nationwide and (2) a national strategy to guide efforts to strengthen airport security. DHS concurred and said TSA is developing the assessment and strategy, but has not yet evaluated the need to assess airport vulnerabilities nationwide.

GAO reported in July 2011 that TSA revised explosives detection requirements for its explosives detection systems (EDS) used to screen checked baggage in January 2010, but faces challenges in deploying EDS that meet these requirements. Deploying systems that meet the 2010 EDS requirements could be difficult given that TSA did not begin deployment of systems meeting the previous 2005 requirements until 2009. As of January 2011 some of the EDS in TSA's fleet detect explosives at the level established in 2005 while the remaining EDS detect explosives at levels established in 1998. Further, TSA does not have a plan to deploy and operate systems to meet the current requirements and has faced challenges in procuring the first 260 systems to meet these requirements. GAO recommended that TSA, among other things, develop a plan to ensure that EDS are operated at the levels in established requirements. DHS agreed and has outlined actions to do so.

Chairman Chaffetz, Ranking Member Tierney, and Members of the Subcommittee:

I appreciate the opportunity to participate in today's hearing to discuss three key layers of aviation security: (1) the Transportation Security Administration's (TSA) behavior-based passenger screening program, (2) airport perimeter and access controls security, and (3) airport checked baggage screening systems.[1] The attempted terrorist bombing of Northwest flight 253 on December 25, 2009, provided a vivid reminder that civil aviation remains an attractive terrorist target and underscores the need for effective passenger screening. According to the President's *National Counterterrorism Strategy* released in June 2011, aviation security and screening is an essential tool in our ability to detect, disrupt, and defeat plots to attack the homeland.[2]

Securing commercial aviation operations remain a daunting task—with hundreds of airports, thousands of aircraft, and thousands of flights daily carrying millions of passengers and pieces of checked baggage. In the almost 10 years that have passed since TSA assumed responsibility for aviation security, TSA has spent billions of dollars and implemented a wide range of initiatives to strengthen the layers of aviation security. However, risks to the aviation system remain.

In addition, while airport operators, not TSA, generally retain direct day-to-day operational responsibility for airport perimeter security and implementing access controls for secure areas of their airports, TSA has responsibility for establishing and implementing measures to improve security in these areas.[3] Criminal incidents involving airport workers using their access privileges to smuggle weapons and drugs into secure areas

[1]TSA's behavior-based passenger screening program is known as the Screening of Passengers by Observation Techniques (SPOT) program.

[2]*National Strategy for Counterterrorism*, (Washington, D.C.: June 28, 2011).

[3]For the purposes of this testimony "secure area" is used generally to refer to areas specified in an airport security program for which access is restricted, including the security identification display areas (SIDA), the air operations areas (AOA), and the sterile areas. While security measures governing access to such areas may vary, in general a SIDA is an area in which appropriate identification must be worn, an AOA is an area providing access to aircraft movement and parking areas, and a sterile area provides passengers access to boarding aircraft and where access is generally controlled by TSA or a private screening entity under TSA oversight. See 49 C.F.R. § 1540.5.

and onto planes have heightened concerns about the risks posed by workers and the security of airport perimeters and access to secure areas.

My statement today discusses the extent to which TSA has taken actions to (1) validate the scientific basis of its behavior-based passenger screening program (referred to as SPOT), (2) strengthen the security of airport perimeters and access controls, and (3) deploy more effective checked baggage screening systems.

This statement is based on our prior work issued from September 2009 through July 2011, and includes selected updates conducted from June 2011 through July 2011 on TSA's efforts to implement our prior recommendations regarding aviation security, including those related to SPOT and airport perimeters and access to secure areas of airports.[4] For our May 2010 report on SPOT, we reviewed relevant literature on behavior analysis by subject matter experts.[5] We conducted field site visits to 15 TSA-regulated airports with SPOT to observe operations and meet with key program personnel.[6] We also interviewed recognized experts in the field, as well as cognizant officials from other U.S. government agencies that utilize behavior analysis in their work. For the updates, we analyzed documentation from TSA on the actions it has taken to implement the recommendations from our May 2010 report,

[4]See 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); GAO, *Aviation Security: Efforts to Validate TSA's Passenger Screening Behavior Detection Program Underway, but Opportunities Exist to Strengthen Validation and Address Operational Challenges*, GAO-10-763 (Washington, D.C.: May 20, 2010); and GAO, *Aviation Security: TSA Has Enhanced Its Explosives Detection Requirements for Checked Baggage, but Additional Screening Actions Are Needed*, GAO-11-740 (Washington, D.C.: July 11, 2011).

[5]National Research Council, *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Assessment* (Washington, D.C.: National Academies Press, 2008). The report's preparation was overseen by the National Academy of Sciences Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals. Although the report addresses broader issues related to privacy and data mining, a senior National Research Council official stated that the committee included behavior detection as a focus because any behavior detection program could have privacy implications.

[6]For the purposes of this testimony, the term "TSA-regulated airport" refers to a U.S. airport operating under a TSA-approved security program and subject to TSA regulation and oversight. See 49 C.F.R. pt. 1542.

including efforts to validate the scientific basis for the program. As part of our efforts to update this information, we analyzed DHS's April 2011 SPOT validation study and discussed its findings with cognizant DHS officials.

For our September 2009 report on TSA efforts to secure airport perimeters and access controls, we examined TSA documents related to risk assessments, airport security programs, and risk management. We also interviewed TSA, airport, and industry association officials and conducted site visits at nine TSA-regulated airports of varying size.[7] We selectively updated the information in the report on risk management in July 2011.

For our July 2011 report on checked baggage systems, we compared requirements for explosives detection systems (EDS) established by TSA in 2010 and compared them to requirements previously established in 2005 and 1998 to determine how they differed.[8] To identify challenges TSA is experiencing in implementing the current EDS acquisition, we analyzed documentation from the Electronic Baggage Screening Program, including the acquisition strategy and risk management plans. We also interviewed TSA program officials regarding their approach to the current EDS acquisition, including revisions to plans and timelines. Our previously published products contain additional details on the scope and methodology, including data reliability, for these reviews.

All of our work was conducted in accordance with generally accepted government auditing standards. These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis of 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. For new information that was based on work not previously reported, we obtained TSA views on our findings and incorporated technical comments where appropriate.

[7]See GAO-09-399.

[8]See GAO-11-740.

Background

The Aviation and Transportation Security Act established TSA as the federal agency with primary responsibility for securing the nation's civil aviation system, which includes the screening of all passenger and property transported by commercial passenger aircraft.[9] At the 463 TSA-regulated airports in the U.S., prior to boarding an aircraft, all passengers, their accessible property, and their checked baggage are screened pursuant to TSA-established procedures, which include passengers passing through security checkpoints where they and their identification documents are checked by transportation security officers (TSO) and other TSA employees or by private sector screeners under TSA's Screening Partnership Program.[10] Airport operators, however, are directly responsible for implementing TSA security requirements, such as those relating to perimeter security and access controls, in accordance with their approved security programs and other TSA direction.

TSA relies upon multiple layers of security to deter, detect, and disrupt persons posing a potential risk to aviation security. These layers include behavior detection officers (BDOs), who examine passenger behaviors and appearances to identify passengers who might pose a potential security risk at TSA-regulated airports;[11] travel document checkers, who examine tickets, passports, and other forms of identification; TSOs responsible for screening passengers and their carry-on baggage at passenger checkpoints, using x-ray equipment, magnetometers, Advanced Imaging Technology, and other devices; random employee screening; and checked baggage screening systems.[12] Other security layers cited by TSA include, among others; intelligence gathering and

[9]See Pub. L. No. 107-71, 115 Stat. 597 (2001). For purposes of this testimony, "commercial passenger aircraft" refers to a U.S. or foreign-based air carrier operating under TSA-approved security programs with regularly scheduled passenger operations to or from a U.S. airport.

[10]Private-sector screeners under contract to and overseen by TSA, and not TSOs, perform screening activities at airports participating in TSA's Screening Partnership Program. According to TSA, 16 airports participate in the program as of July 2011. See 49 U.S.C. § 44920.

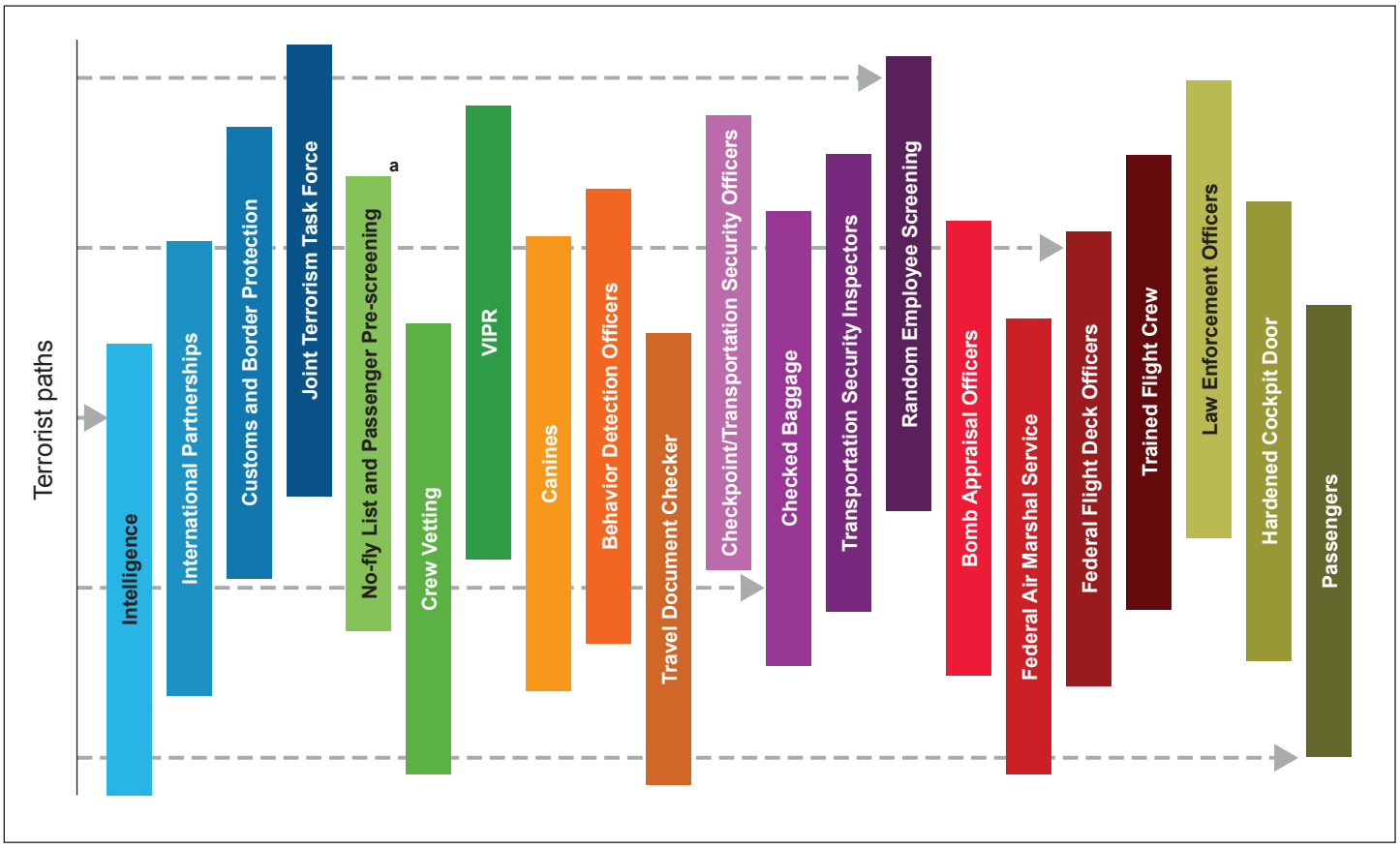
[11]TSA designed SPOT to provide BDOs with a means of identifying persons who may pose a potential security risk at TSA-regulated airports by focusing on behaviors and appearances that deviate from an established baseline and that may be indicative of stress, fear, or deception.

[12]Advanced Imaging Technology screens passengers for metallic and non-metallic threats including weapons, explosives, and other objects concealed under layers of clothing.

analysis; passenger prescreening against terrorist watchlists; random canine team searches at airports; federal air marshals, who provide federal law enforcement presence on selected flights operated by U.S. air carriers; Visible Intermodal Protection Response (VIPR) teams; reinforced cockpit doors; the passengers themselves; as well as other measures both visible and invisible to the public. Figure 1 shows TSA's layers of aviation security. TSA has also implemented a variety of programs and protective actions to strengthen airport perimeters and access to sensitive areas of the airport, including conducting additional employee background checks and assessing different biometric-identification technologies.[13] Airport perimeter and access control security is intended to prevent unauthorized access into secure areas of an airport—either from outside or within the airport complex.

[13]Biometrics are measurements of an individual's unique characteristics, such as fingerprints, irises, and facial characteristics, used to verify identity.

Figure 1: TSA's Layers of Security



Source: TSA.

[a]The No-Fly List is used to identify individuals who are to be prevented from boarding an aircraft while the Selectee List, another aspect of passenger prescreening, is used to identify individuals required to undergo additional screening before being permitted to board an aircraft. The No Fly and Selectee lists are derived from the consolidated terrorist watchlist maintained by the Federal Bureau of Investigation's Terrorist Screening Center.

According to TSA, each one of these layers alone is capable of stopping a terrorist attack. TSA states that the security layers in combination multiply their value, creating a much stronger system, and that a terrorist who has to overcome multiple security layers to carry out an attack is more likely to be preempted, deterred, or to fail during the attempt.

Behavior Detection Program

TSA has taken actions to validate the science underlying its behavior detection program, but more work remains. We reported in May 2010 that TSA deployed SPOT nationwide before first determining whether there was a scientifically valid basis for using behavior and appearance indicators as a means for reliably identifying passengers who may pose a risk to the U.S. aviation system.[14] DHS's Science and Technology Directorate completed a validation study in April 2011 to determine the extent to which SPOT was more effective than random screening at identifying security threats and how the program's behaviors correlate to identifying high-risk travelers.[15] However, as noted in the study, the assessment was an initial validation step, but was not designed to fully validate whether behavior detection can be used to reliably identify individuals in an airport environment who pose a security risk. According to DHS, further research will be needed to comprehensively validate the program.

According to TSA, SPOT was deployed before a scientific validation of the program was completed to help address potential threats to the aviation system, such as those posed by suicide bombers. TSA also stated that the program was based upon scientific research available at the time regarding human behaviors. We reported in May 2010 that approximately 14,000 passengers were referred to law enforcement officers under SPOT from May 2004 through August 2008.[16] Of these passengers, 1,083 were arrested for various reasons, including being illegal aliens (39 percent), having outstanding warrants (19 percent), and possessing fraudulent documents (15 percent). The remaining 27 percent were related to other reasons for arrest. As noted in our May 2010 report, SPOT officials told us that it is not known if the SPOT program has ever resulted in the arrest of anyone who is a terrorist, or who was planning to engage in terrorist-related activity. According to TSA, SPOT referred about 50,000 passengers for additional screening in fiscal year 2010 resulting in about 3,600 referrals to law enforcement officers. These

[14]See GAO-10-763.

[15]See DHS, *SPOT Referral Report Validation Study Final Report Volume I: Technical Report*, (Washington, D.C.: April 5, 2011). DHS's study defines high-risk passengers as travelers that knowingly and intentionally try to defeat the security process including those carrying serious prohibited items, such as weapons; illegal items; such as drugs; or fraudulent documents; or those that were ultimately arrested by law enforcement.

[16]See GAO-10-763.

referrals yielded approximately 300 arrests. Of these 300 arrests, TSA stated that 27 percent were illegal aliens, 17 percent were drug-related, 14 percent were related to fraudulent documents, 12 percent were related to outstanding warrants, and 30 percent were related to other offenses. DHS has requested about $254 million in fiscal year 2012 for the SPOT program, which would support an additional 350 (or 175 full-time equivalent) BDOs. If TSA receives its requested appropriation, TSA will be in a position to have invested about $1 billion in the SPOT program since fiscal year 2007.

A 2008 report issued by the National Research Council of the National Academy of Sciences stated that the scientific evidence for behavioral monitoring is preliminary in nature.[17] The report also noted that an information-based program, such as a behavior detection program, should first determine if a scientific foundation exists and use scientifically valid criteria to evaluate its effectiveness before deployment. The report added that such programs should have a sound experimental basis and that the documentation on the program's effectiveness should be reviewed by an independent entity capable of evaluating the supporting scientific evidence.[18]

As we reported in May 2010, an independent panel of experts could help DHS develop a comprehensive methodology to determine if the SPOT program is based on valid scientific principles that can be effectively applied in an airport environment for counterterrorism purposes. Thus, we recommended that the Secretary of Homeland Security convene an independent panel of experts to review the methodology of the validation study on the SPOT program being conducted to determine whether the study's methodology is sufficiently comprehensive to validate the SPOT program. We also recommended that this assessment include appropriate input from other federal agencies with expertise in behavior detection and relevant subject matter experts.[19] DHS concurred and

[17]Specifically, the report states that the scientific support for linkages between behavioral and physiological markers and mental state is strongest for elementary states, such as simple emotions; weak for more complex states, such as deception; and nonexistent for highly complex states, such as when individuals hold terrorist intent and beliefs.

[18]A study performed by the JASON Program Office raised similar concerns. The JASON Program Office is an independent scientific advisory group that provides consulting services to the U.S. government on matters of defense science and technology.

[19]See GAO-10-763.

stated that its validation study, completed in April 2011, included an independent review of the study with input from a broad range of federal agencies and relevant experts, including those from academia.

DHS's validation study found that SPOT was more effective than random screening to varying degrees. For example, the study found that SPOT was more effective than random screening at identifying individuals who possessed fraudulent documents and identifying individuals who law enforcement officers ultimately arrested.[20] According to DHS's study, no other counterterrorism or screening program incorporating behavior- and appearance-based indicators is known to have been subjected to such a rigorous, systematic evaluation of its screening accuracy. However, DHS noted that the identification of such high-risk passengers was rare in both the SPOT and random tests. In addition, DHS determined that the base rate, or frequency, of SPOT behavioral indicators observed by TSA to detect suspicious passengers was very low and that these observed indicators were highly varied across the traveling public. Although details about DHS's findings related to these indicators are sensitive security information, the low base rate and high variability of traveler behaviors highlights the challenge that TSA faces in effectively implementing a standardized list of SPOT behavioral indicators.

In addition, DHS outlined several limitations to the study. For example, the study noted that BDOs were aware of whether individuals they were screening were referred to them as the result of identified SPOT indicators or random selection. DHS stated that this had the potential to introduce bias into the assessment. DHS also noted that SPOT data from January 2006 through October 2010 were used in its analysis of behavioral indicators even though questions about the reliability of the data exist.[21] In May 2010, we reported weaknesses in TSA's process for maintaining operational data from the SPOT program database. Specifically, the SPOT database did not have computerized edit checks built into the system to review the format, existence, and reasonableness of data. Because of these data-related issues, we reported that

[20]The extent to which SPOT is more effective than random at identifying fraudulent documents and individuals ultimately arrested by law enforcement officers is deemed sensitive security information by TSA.

[21]DHS officials stated that this historical SPOT data was not used in their analysis to determine whether SPOT was more effective than random screening.

meaningful analyses could not be conducted to determine if there is an association between certain behaviors and the likelihood that a person displaying certain behaviors would be referred to a law enforcement officer or whether any behavior or combination of behaviors could be used to distinguish deceptive from nondeceptive individuals. In our May 2010 report, we recommended that TSA establish controls for this SPOT data. DHS agreed and TSA has established additional data controls as part of its database upgrade. However, some of DHS's analysis used SPOT data recorded prior to these additional controls.

The study also noted that it was not designed to comprehensively validate whether SPOT can be used to reliably identify individuals in an airport environment who pose a security risk. The DHS study made recommendations related to strengthening the program and conducting a more comprehensive validation of whether the science can be used for counterterrorism purposes in the aviation environment.[22] Some of these recommendations, such as the need for a comprehensive program evaluation including a cost-benefit analysis, reiterate recommendations made in our prior work. As we reported in March 2011, Congress may wish to consider the study's results in making future funding decisions regarding the program.[23] TSA is currently reviewing the study's findings and assessing the steps needed to address DHS's recommendations. If TSA decides to implement the recommendations in the April 2011 DHS validation study, DHS may be years away from knowing whether there is a scientifically valid basis for using behavior detection techniques to help secure the aviation system against terrorist threats given that the initial study took about 4 years to complete.

Airport Perimeter and Access Controls

TSA has taken actions to strengthen airport perimeter and access controls security, but has not conducted a comprehensive risk assessment or developed a national strategy for airport security. We reported in September 2009 that TSA has implemented a variety of programs and actions since 2004 to improve and strengthen airport

[22]The study made recommendations related to SPOT in three areas: (1) future validation efforts; (2) comparing SPOT with other screening programs; and (3) broader program evaluation issues. TSA designated the specific details of these recommendations sensitive security information.

[23]See GAO, *Opportunities to Reduce Potential Duplication in Government Programs, Save Tax Dollars, and Enhance Revenue*, GAO-11-318SP (Washington, D.C.: Mar. 1, 2011).

perimeter and access controls security, including strengthening worker screening and improving access control technology.[24] For example, to better address the risks posed by airport workers, in 2007 TSA implemented a random worker screening program that has been used to enforce access procedures, such as ensuring workers display appropriate credentials and do not possess unauthorized items when entering secure areas. According to TSA officials, this program was developed to help counteract the potential vulnerability of airports to an insider attack—an attack from an airport worker with authorized access to secure areas. TSA has also expanded its requirements for conducting worker background checks and the population of individuals who are subject to these checks. For example, in 2007 TSA expanded requirements for name-based checks to all individuals seeking or holding airport-issued identification badges and in 2009 began requiring airports to renew all airport-identification media every 2 years. TSA also reported taking actions to identify and assess technologies to strengthen airport perimeter and access controls security, such as assisting the aviation industry and a federal aviation advisory committee in developing security standards for biometric access controls.

However, we reported in September 2009 that while TSA has taken actions to assess risk with respect to airport perimeter and access controls security, it had not conducted a comprehensive risk assessment based on assessments of threats, vulnerabilities, and consequences, as required by DHS's *National Infrastructure Protection Plan* (NIPP).[25] We further reported that without a full depiction of threats, vulnerabilities, and consequences, an organization's ability to establish priorities and make cost-effective security decisions is limited.[26] We recommended that TSA develop a comprehensive risk assessment, along with milestones for completing the assessment. DHS concurred with our recommendation and said it would include an assessment of airport perimeter and access control security risks as part of a comprehensive assessment for the transportation sector—the *Transportation Sector Security Risk*

[24]GAO-09-399.

[25]GAO-09-399. DHS developed the *NIPP* to guide risk assessment efforts and the protection of the nation's critical infrastructure, including airports.

[26]See GAO, *Transportation Security: Comprehensive Risk Assessments and Stronger Internal Controls Needed to Help Inform TSA Resource Allocation*, GAO-09-492 (Washington, D.C.: Mar. 27, 2009).

Assessment (TSSRA). The *TSSRA*, published in July 2010, included an assessment of various risk-based scenarios related to airport perimeter security but did not consider the potential vulnerabilities of airports to an insider attack—the insider threat—which it recognized as a significant issue. In July 2011, TSA officials told us that the agency is developing a framework for insider risk that is to be included in the next iteration of the assessment, which TSA expected to be released at the end of calendar year 2011. Such action, if taken, would meet the intent of our recommendation.

We also recommended that, as part of a comprehensive risk assessment of airport perimeter and access controls security, TSA evaluate the need to conduct an assessment of security vulnerabilities at airports nationwide.[27] At the time of our review, TSA told us its primary measures for assessing the vulnerability of airports to attack were professional judgment and the collective results of joint vulnerability assessments (JVA) it conducts with the Federal Bureau of Investigation (FBI) for select—usually high-risk—airports.[28] Our analysis of TSA data showed that from fiscal years 2004 through 2008, TSA conducted JVAs at about 13 percent of the approximately 450 TSA-regulated airports that existed at that time, thus leaving about 87 percent of airports unassessed.[29] TSA has characterized U.S. airports as an interdependent system in which the security of all is affected or disrupted by the security of the weakest link.

[27]GAO-09-399.

[28]According to TSA officials, JVAs are assessments that teams of TSA special agents and other officials conduct jointly with the FBI, generally, as required by law, every 3 years for airports identified as high risk. See 49 U.S.C. § 44904(a)-(b). See also Pub. L. No. 104-264, § 310, 110 Stat. 3213, 3253 (1996) (establishing the requirement that the Federal Aviation Administration (FAA) and the FBI conduct joint threat and vulnerability assessments). Pursuant to ATSA, responsibility for conducting JVAs transferred from FAA to TSA. For more information on this issue, see GAO-09-399.

[29]From fiscal years 2004 through 2008 TSA conducted 67 JVAs at a total of 57 airports; 10 airports received 2 JVAs. TSA classifies the nation's airports into one of five categories (X, I, II, III, and IV) based on various factors such as the number of take-offs and landings annually, the extent of passenger screening at the airport, and other security considerations. In general, Category X airports have the largest number of passenger boardings and Category IV airports have the smallest. According to TSA data, of the 67 JVAs conducted at 57 airports from fiscal years 2004 through 2008, 58—or 87 percent—were Category X and I airports. Of the remaining 9 assessments, 6 were at Category II airports, 1 at a Category III airport, and 2 at Category IV airports. Since our September 2009 report was issued, the number of TSA-regulated airports has increased from approximately 450 to 463.

However, we reported that TSA officials could not explain to what extent the collective JVAs of specific airports constituted a reasonable systems-based assessment of vulnerability across airports nationwide. Moreover, TSA officials said that they did not know to what extent the 87 percent of commercial airports that had not received a JVA as of September 2009—most of which were smaller airports—were vulnerable to an intentional security breach. DHS concurred with our recommendation to assess the need for a vulnerability assessment of airports nationwide. TSA officials also stated that based on our review they intended to increase the number of JVAs conducted at Category II, III, and IV airports and that the resulting data would assist TSA in prioritizing the allocation of limited resources. Our analysis of TSA data showed that from fiscal year 2004 through July 1, 2011, TSA conducted JVAs at about 17 percent of the TSA-regulated airports that existed at that time, thus leaving about 83 percent of airports unassessed.[30] Since we issued our report in September 2009, TSA had not conducted JVAs at Category III and IV airports.[31] Further, TSA could not tell us to what extent it has studied the need to conduct JVAs of security vulnerabilities at airports nationwide.

We also reported in September 2009 that TSA's efforts to enhance the security of the nation's airports have not been guided by a national strategy that identifies key elements, such as goals, priorities, performance measures, and required resources.[32] To better ensure that airport stakeholders take a unified approach to airport security, we recommended that TSA develop a national strategy for airport security that incorporates key characteristics of effective security strategies, such as measurable goals and priorities. DHS concurred with this recommendation and stated that TSA would implement it by updating the *Transportation Systems-Sector Specific Plan* (TS-SSP), to be released in

[30]From fiscal year 2004 through July 1, 2011, TSA conducted 125 JVAs at 78 airports; 47 airports received more than one JVA during this time period.

[31]From fiscal year 2009 through July 1, 2011, TSA conducted 58 JVAs at a total of 56 airports; 2 airports received 2 JVAs. According to TSA data, of the 58 JVAs conducted, 47—or 88 percent—were at Category X and I airports; 7—12 percent—were conducted at Category II airports. TSA officials told us that since our report in September 2009 they have initiated a semi-annual report process that, in part, included a data analysis of the JVAs conducted at airports for the prior six months. The semi-annual report focuses on airport perimeter, terminal, critical infrastructure, airport operations, and airport services. Beginning in fiscal year 2011 the reports are to be developed on an annual basis. The reports are also used to direct future JVA efforts.

[32]GAO-09-399.

the summer of 2010.[33] In July 2011 TSA officials told us that a pre-publication version of the *TS-SSP* had been sent to Congress on June 29, 2011, and that DHS was in the process of finalizing the *TS-SSP* for publication, but a specific date had not been set for public release.

Checked Baggage Screening Systems

TSA has revised explosives detection requirements for checked baggage screening systems but faces challenges in deploying equipment that meet the requirements. Explosives represent a continuing threat to the checked baggage component of aviation security. TSA deploys EDS and explosives trace detection (ETD) machines to screen all checked baggage transported by U.S. and foreign air carriers departing from TSA-regulated airports in the United States. An EDS uses a computed tomography X-ray source that rotates around a bag, obtaining a large number of cross-sectional images that are integrated by a computer that automatically triggers an alarm when objects with the characteristic of explosives are detected. An ETD machine is used to chemically analyze trace materials after a human operator swabs checked baggage to identify any traces of explosive material. TSA seeks to ensure that checked baggage screening technology is capable of detecting explosives through its Electronic Baggage Screening Program, one of the largest acquisition programs within DHS. Under the program, TSA certifies and acquires systems used to screen checked baggage at 463 TSA-regulated airports throughout the United States. TSA certifies explosives detection-screening technologies to ensure they meet explosives detection requirements developed in conjunction with the DHS Science and Technology Directorate along with input from other agencies, such as the FBI and Department of Defense.

Our July 2011 report addressed TSA's efforts to enhance explosives detection requirements for checked-baggage screening technologies as well as TSA's efforts to ensure that currently deployed and newly acquired explosives detection technologies meet the enhanced requirements.[34] As highlighted in our July 2011 report, requirements for EDSs were established in 1998 and subsequently revised in 2005 and

[33]TSA developed the *TS-SSP* to conform to NIPP requirements, which required sector-specific agencies to develop strategic risk management frameworks for their sectors that aligned with *NIPP* guidance.

[34]See GAO-11-740.

2010 to better address the threats. Currently, checked baggage screening systems are not operating under the 2010 requirements. As of January 2011, some of the EDS in TSA's fleet are detecting explosives at the level established by the 2005 requirements.[35] Meanwhile, other EDS are configured to meet older requirements established in 1998, but include software to meet 2005 requirements. The remaining EDS are configured to meet 1998 requirements but lack the software or both the hardware and software that would enable them to detect at the levels established by the 2005 requirements. TSA plans to implement the revised requirements in a phased approach spanning several years.[36] The first phase, which includes implementation of the 2005 requirements, is scheduled to take years to fully implement and deploying EDS that meet 2010 requirements could prove difficult given that TSA did not begin deployment of EDS meeting 2005 requirements until 2009—4 years later.

We found that TSA did not have a plan to deploy and operate EDS to meet the most recent requirements and recommended, among other things, that TSA develop a plan to deploy EDS that meet the current EDS explosives detection requirements and ensure that new EDS, as well as those already deployed in airports, be operated at the levels established in those requirements. In addition, TSA has faced challenges in procuring the first 260 EDS to meet 2010 requirements. For example, due to the danger associated with certain explosives, TSA and DHS encountered challenges safely developing simulants and collecting data on the explosives' physical and chemical properties needed by vendors and agencies to develop detection software and test EDS prior to the current acquisition. Also, TSA's decision to pursue EDS procurement complicated both the data collection and procurement efforts, which resulted in a delay of over 7 months for the current acquisition. We recommended that TSA complete data collection for each phase of the 2010 EDS requirements prior to pursuing EDS procurements that meet those requirements to help TSA avoid additional schedule delays.

[35]TSA has designated the number of EDS at the 2005 requirement level sensitive security information.

[36]The specific details included in the 2010 EDS requirements, such as the physical characteristics and minimum masses of each of the explosive types that EDS machines must detect, are classified.

Our report also examined other key issues such as the extent to which TSA's approach to its current EDS acquisition meets best practices for schedules and cost estimates and included a review of TSA's plans for potential upgrades of deployed EDSs. The report contained six recommendations to TSA, including that the agency develop a plan to ensure that new EDSs, as well as those EDSs currently deployed in airports, operate at levels that meet revised requirements. DHS concurred with all of the recommendations and has subsequently outlined actions to implement them.

Chairman Chaffetz, Ranking Member Tierney, and Members of the Subcommittee, this concludes my statement. I look forward to answering any questions that you may have at this time.

GAO Contact and Staff Acknowledgments

For questions about this statement, please contact Stephen M. Lord 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 statement. Individuals making key contributions to this testimony are David M. Bruno, Glenn Davis, and Steve Morris, Assistant Directors; Scott Behen; Ryan Consaul; Barbara Guffy; Tom Lombardi; Lara Miklozek; and Doug Sloane.

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