United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Oversight, Investigations, and Management, Committee on Homeland Security, House of Representatives

For Release on Delivery
Expected at 9:30 a.m. EDT
Friday, September 16, 2011

AVIATION SECURITY

TSA Has Made Progress, but Additional Efforts Are Needed to Improve Security

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

September 16, 2011

AVIATION SECURITY

TSA Has Made Progress, but Additional Efforts Are Needed to Improve Security

GAO Accountability * Integrity * Reliability

Highlights

Highlights of GAO-11-938T, a testimony before the Subcommittee on Oversight, Investigations, and Management, Committee on Homeland Security, 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 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. Two 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; and (2) airport perimeter and access controls security. This testimony provides information on the extent to which TSA has taken actions to validate the scientific basis of SPOT and strengthen airport perimeter security. This statement is based on prior products GAO issued from September 2009 through September 2011 and selected updates in August and September 2011. To conduct the updates, 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 and airport perimeter and access control security efforts. DHS and TSA generally concurred with the recommendations and have actions under way to address them.

View GAO-11-938T. For more information, contact Stephen M. Lord at (202) 512-8777 or lords@gao.gov.

What GAO Found

DHS completed an initial study in April 2011 to validate the scientific basis of the SPOT program; however, additional work remains to fully validate the program. In May 2010, GAO reported 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. TSA is pilot testing revised program procedures at Boston-Logan airport in which behavior detection officers will engage passengers entering screening in casual conversation to help determine suspicious behaviors. TSA plans to expand this pilot program in the fall of 2011. GAO recommended in May 2010 that DHS, as part of its validation study, assess the methodology to help ensure the validity of the SPOT program. DHS concurred and stated that the study included an independent review with a broad range of agencies and experts. The study found that SPOT was more effective than random screening to varying degrees. 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 also noted that additional work was needed to comprehensively validate the program. TSA officials are assessing the actions needed to address the study's recommendations but do not have time frames for completing this work.

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 had 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 for security by TSA in 2009. GAO recommended that TSA develop (1) a comprehensive risk assessment and evaluate the need to conduct airport vulnerability assessments nationwide and (2) a national strategy to guide efforts to strengthen airport security. DHS concurred and TSA stated that the *Transportation Sector Security Risk Assessment*, issued in July 2010, was to provide a comprehensive risk assessment of airport security. However, this assessment did not consider the potential vulnerabilities of airports to an insider attack—an attack from an airport worker with authorized access to secure areas. In August 2011, TSA reported that transportation security inspectors conduct vulnerability assessments annually at all commercial airports, including an evaluation of perimeter security. GAO has not yet assessed the extent to which inspectors consistently conduct vulnerability assessments. TSA also updated the *Transportation Systems-Sector Specific Plan*, which summarizes airport security program activities. However, the extent to which these activities were guided by measurable goals and priorities, among other things, was not clear. Providing such additional information would better address GAO's recommendation.

Chairman McCaul, Ranking Member Keating, and Members of the Subcommittee:

I appreciate the opportunity to participate in today's hearing at Boston-Logan International Airport to discuss two key layers of aviation security: the Transportation Security Administration's (TSA) behavior-based passenger screening program and airport perimeter and access controls.[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 the 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. For fiscal year 2011, TSA had about 54,800 personnel and its budget authority was about $7.7 billion. However, risks to the aviation system remain. Earlier this month, we reported on the progress made in securing the aviation system in the 10 years since the September 11, 2001, attacks and the work that still remains.[3]

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

[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]See GAO, *Department of Homeland Security: Progress Made and Work Remaining In Implementing Homeland Security Missions 10 Years After 9/11*, GAO-11-881 (Washington, D.C.: Sept. 7, 2011).

security in these areas.[4] Criminal incidents involving airport workers using their access privileges to smuggle weapons and drugs into secure areas and onto planes have heightened concerns about the risks posed by workers and the security of airport perimeters and access to secured 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) and (2) strengthen the security of airport perimeters and access controls.

This statement is based on our prior products issued from September 2009 through September 2011, and includes selected updates conducted in August and September 2011 on TSA's efforts to implement our prior recommendations regarding SPOT and airport perimeters and access to secure areas of airports.[5] For our May 2010 report on SPOT, we reviewed relevant literature on behavior analysis by subject matter experts.[6] We conducted field site visits to 15 TSA-regulated airports with

[4]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.

[5]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); *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); *Aviation Security: TSA Has Taken Actions to Improve Security, but Additional Efforts Remain*, GAO-11-807T (Washington, D.C.: Jul. 13, 2011); and GAO-11-881.

[6]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.

SPOT to observe operations and meet with key program personnel.[7] 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, 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.[8] For the updates, we analyzed documentation from TSA on actions it has taken to implement recommendations from our 2009 report, including efforts to conduct a comprehensive risk assessment and evaluate the need to conduct an assessment of security vulnerabilities at airports nationwide, and to develop a national strategy for airport perimeters and access controls security that identifies key elements such as goals and priorities. As part of our efforts to update this information, we analyzed TSA data on the number of vulnerability assessments conducted at airports from fiscal year 2004 through July 1, 2011, by airport. More detailed information on our scope and methodology can be found in our prior reports.

All of our work was conducted in accordance with generally accepted government auditing standards.

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

[7]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.

[8]See GAO-09-399.

property transported by commercial passenger aircraft.[9] At the 463 TSA-regulated airports in the United States, 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 (BDO), who examine passenger behaviors and appearances to identify passengers who might pose a potential security risk at TSA-regulated airports;[11] TSA has selectively deployed about 3,000 BDOs to 161 of 463 TSA-regulated airports in the United States, including Boston-Logan airport where the program was initially deployed in 2003. Other security layers include 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] Additional layers cited by TSA include, among others, intelligence

[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. See 49 U.S.C. § 44920. According to TSA, 16 airports participated in the program as of July 2011.

[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.

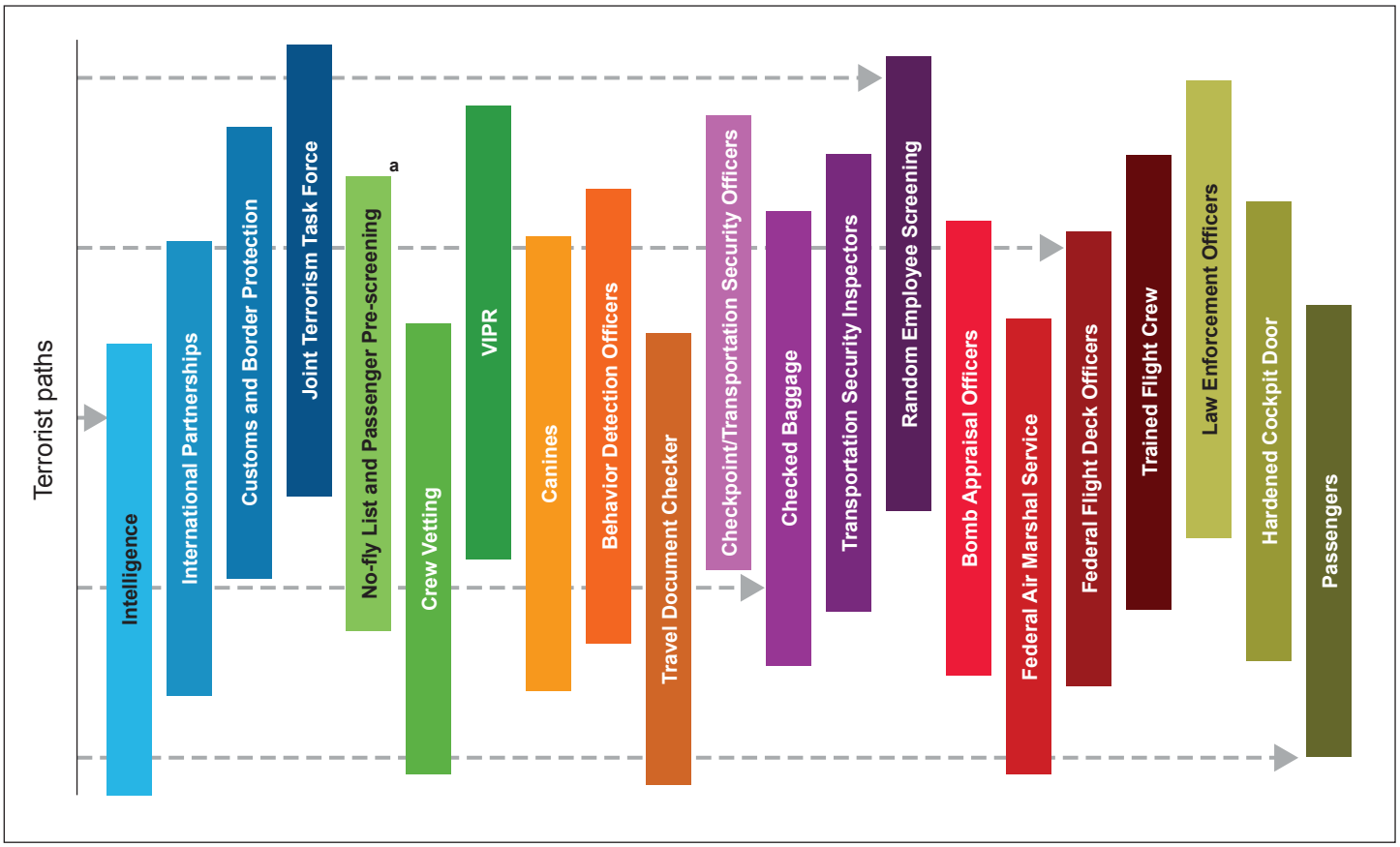
[12]Advanced Imaging Technology screens passengers for metallic and non-metallic threats including weapons, explosives, and other objects concealed under layers of clothing.

gathering and 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.[13] 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.[14] 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]Working alongside local security and law enforcement officials, VIPR teams conduct a variety of security tactics to introduce unpredictability and deter potential terrorist actions, including random high-visibility patrols at mass transit and passenger rail stations and conducting passenger and baggage screening operations using specially trained behavior detection officers and a varying combination of explosive detection canine teams and explosives detection technology.

[14]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 pre-empted, deterred, or to fail during the attempt.

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.[15] 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.[16] 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, additional work 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.[17] 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 arrested for other reasons. As noted in our May 2010 report, SPOT officials told us that it is not known if the SPOT program has resulted in the arrest of anyone who is a terrorist, or who was planning to engage in terrorist-related activity. According to TSA, in fiscal year 2010, SPOT referred about 50,000 passengers for additional screening and about 3,600 referrals to law enforcement officers. The referrals to law enforcement officers yielded approximately 300 arrests. Of these 300 arrests, TSA stated that 27 percent were illegal aliens, 17 percent were

[15]See GAO-10-763.

[16]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.

[17]See GAO-10-763.

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 for 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.

According to TSA, as of August 2011, TSA is pilot testing revised procedures for BDOs at Boston-Logan airport to engage passengers entering screening in casual conversation to help determine suspicious behaviors. According to TSA, after a passenger's travel documents are verified, a BDO will briefly engage each passenger in conversation. If more information is needed to help determine suspicious behaviors, the officer will refer the passenger to a second BDO for a more thorough conversation to determine if additional screening is needed. TSA noted that these BDOs have received additional training in interviewing methods. TSA plans to expand this pilot program to additional airports in the fall of 2011.

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.[18] 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.[19] According to the report, a terrorist's desire to avoid detection makes information-gathering techniques, such as asking what a person has done, is doing, or plans to do, highly unreliable. Using these techniques to elicit information could also have definite privacy

[18]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.

[19]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.

implications. These findings, in particular, may be important as TSA moves forward with its pilot program to expand BDOs' use of conversation and interviews with all passengers entering screening.

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 was 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.[20] DHS concurred and 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.[21] 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.

[20]See GAO-10-763.

[21]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.

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.[22] 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. In another example, BDOs could not input all behaviors observed in the SPOT database because the database limited entry to eight behaviors, six signs of deception, and four types of prohibited items per passenger referred for additional screening. Because of these data-related issues, we reported that meaningful analyses could not be conducted at that time 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 for this study used SPOT data recorded prior to these additional controls being implemented.

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.[23] Some of these recommendations, such as the need for a comprehensive program evaluation including a cost-benefit analysis, reiterate recommendations

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

[23]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.

made in our May 2010 report. TSA is currently reviewing the study's findings and assessing the steps needed to address DHS's recommendations but does not have time frames for completing this work. 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 the broad scope of the additional work and related resources identified by DHS for addressing the recommendations. Thus, as we reported in March 2011, Congress may wish to consider the study's results in making future funding decisions regarding the program.[24]

TSA Has Taken Actions to Strengthen Airport Perimeter and Access Controls Security, but Issues Remain

We reported in September 2009 that TSA has implemented a variety of programs and actions since 2004 to improve and strengthen airport perimeter and access controls security, including strengthening worker screening and improving access control technology.[25] For example, to better address the risks posed by airport workers, in 2007 TSA implemented a random worker screening program that was 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.

[24]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).

[25]GAO-09-399.

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).[26] 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.[27] 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 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.[28] 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

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

[27]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).

[28]GAO-09-399.

select—usually high-risk—airports.[29] 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.[30] 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. 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 2009 report recommendation to assess the need for a vulnerability assessment of airports nationwide, and TSA officials stated that based on our review they intended to increase the number of JVAs conducted at Category II, III, and IV airports and use the resulting data to assist 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.[31]

[29]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 every three years, or more frequently, as necessary, at each airport determined to be high risk). Pursuant to ATSA, responsibility for conducting JVAs transferred from FAA to TSA. For more information on this issue, see GAO-09-399.

[30]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.

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

Since we issued our report in September 2009, TSA had not conducted JVAs at Category III and IV airports.[32] TSA stated that the TSSRA is to provide a comprehensive risk assessment of airport security, but could not tell us to what extent it has studied the need to conduct JVAs of security vulnerabilities at airports nationwide. Additionally, in August 2011 TSA reported that its national inspection program requires that transportation security inspectors conduct vulnerability assessments at all commercial airports, which are based on the joint vulnerability assessment model. According to TSA, every commercial airport in the United States receives a security assessment each year, including an evaluation of perimeter security and access controls. We have not yet assessed the extent to which transportation security inspectors consistently conduct vulnerability assessments based on the joint vulnerability model. Providing additional information on how and to what extent such security assessments have been performed would more fully address our recommendation.

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.[33] 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 the summer of 2010.[34] TSA provided a copy of the updated plan to

[32]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 6 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.

[33]GAO-09-399.

[34]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.

congressional committees in June 2011 and to us in August 2011. We reviewed this plan and its accompanying aviation model annex and found that while the plan provided a high-level summary of program activities for addressing airport security such as the screening of workers, the extent to which these efforts would be guided by measurable goals and priorities, among other things, was not clear. Providing such additional information would better address the intent of our recommendation.

Chairman McCaul, Ranking Member Keating, 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 and Steve Morris, Assistant Directors; Ryan Consaul; Barbara Guffy; Tracey King; Tom Lombardi; and Lara Miklozek.

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