United States Government Accountability Office

GAO

Testimony

Before the Committee on Oversight and Government Reform and Committee on Transportation and Infrastructure, House of Representatives

For Release on Delivery
Expected at 1:30 p.m. EDT
Monday, March 26, 2012

TRANSPORTATION SECURITY ADMINISTRATION

Progress and Challenges Faced in Strengthening Three Key Security Programs

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

March 26, 2012

TRANSPORTATION SECURITY ADMINISTRATION

Progress and Challenges Faced in Strengthening Three Key Security Programs

GAO Accountability * Integrity * Reliability

Highlights

Highlights of GAO-12-541T, a testimony before the Committee on Oversight and Government Reform and Committee on Transportation and Infrastructure, House of Representatives

Why GAO Did This Study

DHS and TSA have made some notable achievements in securing the nation's transportation systems since the terrorist attacks of September 11, 2001, but in recent years, GAO reported that DHS has experienced challenges in managing its efforts including fielding programs prior to determining their effectiveness or completing cost-benefit analyses. This testimony focuses on, among other things, DHS and TSA's progress and challenges in implementing three key security programs: SPOT, AIT, and TWIC. This testimony is based on reports and testimonies issued from November 2009 through March 2012, and includes selected updates conducted from February through March 2012. To conduct these updates, GAO obtained information on the current status of the programs and progress made related to the implementation of recommendations contained in prior GAO reports.

What GAO Recommends

GAO is not making any new recommendations. In prior work, GAO made recommendations to address challenges related to assessing SPOT effectiveness as well as AIT utilization. GAO also recommended that DHS assess TWIC effectiveness and use this assessment to evaluate the costs, benefits, and risks of TWIC. DHS and TSA concurred and have actions underway to address the recommendations.

View GAO-12-541T. For more information, contact Steve Lord at (202) 512-4379 or lords@gao.gov.

What GAO Found

The Transportation Security Administration (TSA) relies on layers of security encompassing personnel, processes, and technology to deter, detect, and disrupt persons posing a potential risk to aviation security. The Screening of Passengers by Observation Techniques (SPOT) program consists of about 3,000 behavior detection officers (BDO) who examine passengers to identify those who might pose a security risk at over 160 TSA-regulated airports. Advanced Imaging Technology (AIT)—full body scanners—are intended to help TSA staff detect explosives and other threats on passengers. Also, TSA and the U.S. Coast Guard manage the Transportation Worker Identification Credential (TWIC) program, which employs a federally-sponsored credential in an effort to enhance access controls at Maritime Transportation Security Act regulated facilities and vessels. The Department of Homeland Security (DHS) and TSA have made progress and faced challenges in implementing these programs.

SPOT. Additional DHS and TSA actions are needed to validate SPOT and to establish performance measures. GAO reported in May 2010 that TSA deployed SPOT nationwide before determining whether it had a scientifically valid basis. GAO recommended that DHS convene an independent panel of experts to review DHS's efforts to validate SPOT and determine whether the methodology used was sufficiently comprehensive. DHS agreed and completed this study in April 2011. The study found that SPOT was more effective than random screening to varying degrees; however, as noted in the study, the assessment was an initial validation step and was not designed to fully validate whether BDOs can reliably identify individuals who pose a security risk. According to DHS, additional work will be needed to validate SPOT. Also, GAO reported that TSA has implemented certain performance measures to assess the program, but has not fielded outcome-oriented performance measures—which track progress by documenting the beneficial results of programs—to help assess SPOT's contribution to improving aviation security. In May 2010, GAO recommended and TSA agreed that to better measure SPOT's effectiveness and evaluate the performance of BDOs, TSA should establish a plan to develop outcome-oriented performance measures.

AIT. DHS accelerated the deployment of AIT to identify threat materials and to provide enhanced security benefits compared to metal detectors. In January 2012, GAO reported instances where AIT units were not being used, raising questions about the cost-effectiveness of this acquisition. For example, data GAO collected from March 2010 through February 2011 on all deployed AIT units showed that some deployed units were not used regularly, decreasing their potential security benefit. GAO recommended and TSA agreed to study AIT utilization and address the extent to which currently deployed units are used.

TWIC. As of March 2012, the TWIC program has enrolled over 2.1 million maritime workers and DHS has established TWIC-related processes and controls. In May 2011, GAO recommended that DHS conduct an assessment that includes addressing internal control weaknesses and evaluate whether use of TWIC would further enhance the security posture. GAO also recommended that this assessment be used to evaluate the costs, benefits, and security risks of the TWIC program prior to requiring its use. DHS agreed and, as of March 2012, reports that it is further evaluating the TWIC program.

Chairmen Issa and Mica, Ranking Members Cummings and Rahall, and Members of the Committees:

I am pleased to be here today to discuss our past work examining the Transportation Security Administration's (TSA) progress and challenges in improving transportation security. 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. 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. Likewise, securing operations at our nation's maritime ports requires balancing security to address potential threats while facilitating the flow of people and goods that are critical to the U.S. economy and international commerce. Transportation systems and facilities are vulnerable and difficult to secure given their size, easy accessibility, large number of potential targets, and proximity to urban areas.

As noted in our 9/11 Anniversary report, the terrorist attacks of September 11, 2001, led to profound changes in government agendas, policies, and structures to confront homeland security threats facing the nation.[1] As highlighted in this report, the Department of Homeland Security (DHS) and TSA have made notable achievements since these attacks, including developing programs and technologies to screen passengers, and control access to secured airport areas and port facilities, yet challenges remain.

My testimony today focuses on DHS and TSA's progress and related challenges in implementing three key programs:

- Screening of Passengers by Observation Techniques (SPOT) program—A TSA-designed program to provide behavior detection officers (BDO) 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.

[1] 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).

- Advanced Imaging Technology (AIT)—a technology used to screen passengers in the nation's airports.
- Transportation Worker Identification Credential (TWIC) program—a DHS program that requires maritime workers to complete background checks and obtain a biometric identification card to gain unescorted access to secure areas of regulated maritime facilities.

This statement is based on our reports and testimonies issued from March 2010 through March 2012 related to TSA's efforts to manage transportation security programs as well as selected updates, conducted from February 2012 through March 2012, related to the current status of the SPOT and TWIC programs and progress made on implementing previous GAO recommendations aimed at correcting program deficiencies.[2] For our past work, we reviewed applicable laws, regulations, and policies. We also conducted interviews with DHS component program managers and Science and Technology Directorate officials to discuss issues related to individual programs, visited selected airports to observe operations and meet with key program personnel, analyzed available data from relevant program databases, and used other methodologies. As part of our TWIC work, our investigators conducted covert testing at enrollment center(s) to identify whether individuals providing fraudulent information could acquire an authentic TWIC, and at maritime ports with facilities regulated pursuant to the Maritime Transportation Security Act of 2002 (MTSA) to identify security vulnerabilities and program control deficiencies. More detailed information on the scope and methodology from our previous work can be found within each specific report. For the updates, we obtained budget information from TSA and information on its efforts to conduct a cost-benefit analysis of the SPOT program, as well as efforts to address TWIC program internal control weaknesses, among other things. We conducted this work in accordance with generally accepted government auditing

[2] We are evaluating the results of a TWIC pilot and the DHS report on the results of the TWIC pilot that was submitted to the House Committees on Homeland Security and Transportation and Infrastructure and the Senate Committees on Commerce, Science, and Transportation and Homeland Security and Governmental Affairs, as well as to the Comptroller General, on February 27, 2012 pursuant to section 802 of the Coast Guard Authorization Act of 2010. See Pub.L. No. 111-281, 124 Stat. 2905, 2989-90 (2010). We plan to issue a report with the results from this work by the end of 2012. At the request of the House Committee on Transportation and Infrastructure we are initiating a review of the SPOT program which will examine TSA efforts to address some of the limitations identified in earlier DHS and GAO studies. We plan to issue a report with the results from this work in 2013.

standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We conducted our related investigative work in accordance with standards prescribed by the Council of the Inspectors General on Integrity and Efficiency.

Background

The Aviation and Transportation Security Act (ATSA) established TSA as the federal agency with primary responsibility for securing the nation's civil aviation system, which includes the screening of all passengers and property transported from and within the United States by commercial passenger aircraft.[3] In accordance with ATSA, all passengers, their accessible property, and their checked baggage are screened pursuant to TSA-established procedures at the 446 airports presently regulated for security by TSA. These procedures generally provide, among other things, that passengers pass through security checkpoints where they and their identification documents, and accessible property, are checked by transportation security officers (TSO), other TSA employees, or by private-sector screeners under TSA's Screening Partnership Program.[4] Airport operators, however, also have direct responsibility 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 BDOs, who examine airport passenger behaviors and appearances to identify passengers who might pose a potential security risk at TSA-regulated airports; travel document checkers, who examine tickets, passports, and other forms of identification; TSOs responsible for screening passengers and their carry-on baggage at passenger

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

[4] Private-sector screeners, employed by an entity under contract to and overseen by TSA, and not TSOs, perform screening activities at the 16 airports currently participating in TSA's Screening Partnership Program as of March 2012. See 49 U.S.C. § 44920.

checkpoints, using X-ray equipment, magnetometers, AIT, and other devices; random employee screening; and checked-baggage screening.[5]

MTSA required the Secretary of Homeland Security to prescribe regulations preventing individuals from having unescorted access to secure areas of MTSA-regulated facilities and vessels unless they possess a biometric transportation security card[6] and are authorized to be in such an area.[7] Pursuant to MTSA, the Secretary shall issue such biometric transportation security cards to eligible individuals unless the Secretary determines that an applicant poses a security risk warranting denial of the card. The TWIC program is designed to implement these biometric maritime security card requirements. The program requires maritime workers to complete background checks to obtain a biometric identification card and be authorized to be in the secure area by the owner/operator in order to gain unescorted access to secure areas of MTSA-regulated facilities and vessels. Within DHS, TSA and the U.S. Coast Guard manage the TWIC program.

A federal regulation (known as the credential rule) issued in January 2007 sets a compliance deadline, subsequently extended to April 15, 2009, whereby each maritime worker would be required to hold a TWIC in order to obtain unescorted access to secure areas of MTSA-regulated facilities and vessels.[8] A second rule, the card reader rule, is currently under development and is expected to address how the access-control technologies, such as biometric card readers, are to be used for confirming the identity of the TWIC holder against the biometric information on the TWIC. TSA conducted a pilot program ending on May 31, 2011, testing the use of TWICs with biometric card readers to help

[5] AIT, commonly referred to as body scanners, produces images of the body to screen passengers for metallic and nonmetallic threats including weapons, explosives, and other objects concealed under layers of clothing.

[6] Biometrics refers to technologies that measure and analyze human body characteristics—such as fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements—for authentication purposes.

[7] See Pub. L. No. 107-295, § 101, 116 Stat. 2064, 2073-74 (2002) (codified as amended at 46 U.S.C. § 70105).

[8] The credential rule established that all maritime workers requiring unescorted access to secure areas of MTSA-regulated facilities and vessels were expected to hold TWICs by September 25, 2008. See 72 Fed. Reg. 3,492 (Jan. 25, 2007). The final compliance date was subsequently extended to April 15, 2009. See 73 Fed. Reg. 25,562 (May 7, 2008).

inform the development of a second TWIC regulation, among other purposes.

Additional DHS and TSA Actions Needed to Validate TSA's Behavior-Based Screening Program, Establish Performance Measures, and Assess Costs and Benefits

TSA developed the SPOT program in an effort to respond to potential threats to aviation security by identifying individuals who may pose a threat to aviation security, including terrorists planning or executing an attack who were not likely to be identified by TSA's other screening security measures. This program was designed to focus on identifying behaviors and appearances that deviate from an established baseline and that may be indicative of stress, fear, or deception. As we reported in September 2011, TSA had deployed about 3,000 BDOs to about 160 of the approximately 446 TSA-regulated airports in the United States at which passengers and their property are subject to TSA-mandated screening procedures.[9] The following describes progress achieved and challenges faced by TSA in validating the science underlying the SPOT program, developing performance measures, and conducting cost-benefit analysis of SPOT.

Validation efforts. TSA has taken actions to validate the science underlying its behavior detection program, but more work remains. In May 2010 we reported 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.[10] We recommended that DHS convene an independent panel of experts to review DHS's efforts to validate the program and determine whether the validation methodology used was sufficiently comprehensive. DHS concurred with our recommendation, and its 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

[9] See GAO, *Aviation Security: TSA Has Made Progress, but Additional Efforts Are Needed to Improve Security*, GAO-11-938T (Washington, D.C.: Sept. 16, 2011). In our September 2011 testimony, we cited 463 TSA-regulated airports. TSA has subsequently reduced that number to 446.

[10] See 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).

identifying high-risk travelers.[11] The study found that SPOT was more effective than random screening to varying degrees. However, as noted in the study, the assessment was an initial validation step and 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. In addition, DHS outlined several limitations to the study. For example, the study noted that BDOs were aware that individuals they were screening were referred to them as the result of BDO-identified SPOT indicators or random selection. DHS stated that this had the potential to introduce bias into the assessment, and that additional work would be needed to comprehensively validate the program.

DHS's study made recommendations related to the need for further validation efforts, comparing SPOT with other screening programs, and broader program evaluation issues, some of which echoed recommendations we made in May 2010. DHS's recommendations are intended to help the program conduct a more comprehensive validation of whether the science can be used for counterterrorism purposes in the aviation environment. Given the broad scope of the additional work and needed resources identified by DHS for addressing the recommendations, it could take several years to complete. Officials further stated that it is undertaking actions to address some of these recommendations, such as conducting additional analysis of the program's behaviors and associated SPOT scoring system in coordination with DHS's Science and Technology Directorate.[12] According to TSA, a refined list of the behaviors and appearances used in the SPOT program to identify high-risk passengers will be completed by mid-2012. TSA is taking actions to refine the program, but questions related to the program's validity will remain until TSA demonstrates that using behavior detection techniques can help secure the aviation system against terrorist threats.

[11] See DHS, *SPOT Referral Report Validation Study Final Report Volume I: Technical Report* (Washington, D.C.: Apr. 5, 2011). DHS's study defines high-risk passengers as travelers who 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 who were ultimately arrested by law enforcement.

[12] TSA developed a scoring system to help determine which passengers exhibited enough SPOT behaviors to be referred to secondary screening or to law enforcement officers for additional screening, or both.

According to TSA, as part of its SPOT improvement efforts, TSA is pilot testing revised procedures for BDOs at Boston-Logan and Detroit International Airports 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. We will be assessing this pilot as part of a follow-on review of the SPOT program requested by the Chairman of the House Transportation and Infrastructure Committee and plan to report on the results in 2013.

Performance measures. Our work on TSA's behavior detection program has underscored the importance of developing sound measures to evaluate the effectiveness of TSA security programs. The Office of Management and Budget (OMB) encourages the use of outcome measures—which track progress toward a strategic goal by documenting the beneficial results of programs—because they are more meaningful than output measures, which tend to be more process oriented or a means to an end.[13] Congress also needs information on whether and in what respects a program is working well or poorly to support its oversight of agencies and their budgets. As we reported in May 2010, TSA had

[13] DHS's *National Infrastructure Protection Plan* (Washington, D.C.: June 2006), internal controls standards, and our previous work on program assessment state that performance metrics and associated program evaluations are needed to determine if a program works and to identify adjustments that may improve its results. The NIPP includes a risk management framework that consists of six steps, which closely reflects GAO's risk management framework. (See GAO, *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*, GAO-06-91 (Washington, D.C.: Dec. 15, 2005). Like GAO's framework, the NIPP's risk management framework is a repetitive process that continuously uses the results of each step to inform the activities in both subsequent and previous steps over time. The NIPP risk management framework is designed to produce a systematic and comprehensive understanding of risk and ultimately provide for security investments based on this knowledge of risk.

established output-based performance measures[14] for the SPOT program, such as the number of SPOT referrals to law enforcement officers and subsequent arrests; however, it had not fielded outcome-oriented performance measures, such as identifying individuals who may pose a threat to the transportation system, to evaluate the effectiveness of the SPOT program. With such outcome measures, TSA could more fully assess SPOT's contribution to improving aviation security.

As noted in our May 2010 report, SPOT officials told us that it was not known if the SPOT program 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 made 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 drug related, 14 percent were related to fraudulent documents, 12 percent were related to outstanding warrants, and 30 percent were related to other offenses. As highlighted in our May 2010 report, we examined the travel of key individuals allegedly involved in six terrorist plots that have been uncovered by law enforcement agencies. We determined that at least 16 of the individuals allegedly involved in these plots moved through 8 different airports where the SPOT program had been implemented. In total, these individuals moved through SPOT airports on at least 23 different occasions.[15]

In May 2010, we recommended that to better measure the effectiveness of the program and evaluate the performance of BDOs, TSA should

[14] According to OMB Circular No. A-11, outputs describe the level of activity that will be provided over a period of time, including a description of the characteristics (e.g., timeliness) established as standards for the activity. They also refer to the internal activities of a program (i.e., the products and services delivered). Output measures help determine the extent to which an activity was performed as planned. Outcome-related measures are more robust measures because they provide a more comprehensive assessment of the success of the agency's efforts, as stated in DHS's 2009 NIPP.

[15] For example, according to Department of Justice documents, in December 2007 an individual who later pleaded guilty to providing material support to Somali terrorists boarded a plane at the Minneapolis-Saint Paul International Airport en route to Somalia to join terrorists there. Similarly, in August 2008 an individual who later pleaded guilty to providing material support to al-Qaeda boarded a plane at Newark Liberty International Airport en route to Pakistan to receive terrorist training to support his efforts to attack the New York subway system.

establish a plan that includes objectives, milestones, and time frames to develop outcome-oriented performance measures.[16] DHS concurred with our recommendation while noting that it is difficult to establish measures for a deterrence-based program. According to TSA, the agency has recently developed a metrics framework, which includes process measures, output measures, and outcome measures, that will allow SPOT programs at each airport to measure their improvement year by year. After the framework is validated by DHS's Science and Technology Directorate and subject matter experts, TSA expects to roll out this metrics framework as part of TSA's general performance management system in the fourth quarter of fiscal year 2012. We plan to assess this framework as part of our recently initiated review of SPOT.

Cost-Benefit Analysis. As we reported in May 2010, TSA did not complete a cost-benefit analysis before deploying the SPOT program. According to the DHS National Infrastructure Protection Plan, security strategies should be informed by, among other things, a risk assessment that includes threat, vulnerability, and consequence assessments; information such as cost-benefit analyses to prioritize investments; and performance measures to assess the extent to which a strategy reduces or mitigates the risk of terrorist attacks.[17] Our prior work has shown that cost-benefit analyses help congressional and agency decision makers assess and prioritize resource investments and consider potentially more cost-effective alternatives, and that without this ability, agencies are at risk of experiencing cost overruns, missed deadlines, and performance shortfalls.[18]

In May 2010, we reported that TSA did not conduct such an analysis of SPOT prior to full-scale nationwide deployment, and we recommended that it do so, including a comparison of the SPOT program with other security screening programs, such as random screening, or already existing security measures. DHS concurred with our recommendation and noted that TSA was developing an initial cost-benefit analysis. However, it was not clear from DHS's comments whether its cost-benefit analysis

[16] GAO-10-763.

[17] DHS, *National Infrastructure Protection Plan*. In 2009, DHS issued an updated plan that replaced the one issued in 2006.

[18] See GAO, *Homeland Security: DHS and TSA Acquisition and Development of New Technologies*, GAO-11-957T (Washington, D.C.: Sept. 22, 2011).

would include a comparison of the SPOT program with other TSA security screening programs and existing security measures as we recommended. As of March 2012, TSA has not conducted a cost-benefit analysis, which could help the agency establish the value of the program relative to other layers of aviation security. Moreover, a cost-benefit analysis could also be useful in considering future program growth. The program's budget has increased from $198 million in fiscal year 2009 to a requested $227 million in fiscal year 2013, a 15 percent increase over 5 years. In March 2012, TSA officials stated that TSA has developed a "risk and cost analysis framework," which has been applied to several different TSA programs, such as its AIT. TSA is refining the framework in order to complete the risk and cost analysis work for SPOT BDOs, which could provide TSA management with additional information on whether its BDO allocation is a prudent investment. We will be assessing this issue as part of our recently initiated review of SPOT.

Full-Body Scanners Not Fully Utilized at Some Airports

As we reported in March 2010, 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 AIT to identify materials such as those used in the attempted Christmas Day bombing.[19] According to TSA officials, AIT was to provide enhanced security benefits compared to walk-through metal detectors, such as enhanced detection capabilities for identifying nonmetallic threat objects and liquids.

In January 2012, we issued a classified report on TSA's procurement and deployment of AIT, commonly referred to as full body scanners, at airport checkpoints.[20] As of March 2012, TSA has deployed about 640 AIT units to 165 TSA-regulated airports. Among other things, we reported instances where AIT units were not being used, which raised questions about the

[19] See GAO-10-484T. The other four actions include modifying the criteria used to create terrorist watch lists, establishing a partnership between DHS and the Department of Energy and its national laboratories to develop new technologies to deter threats to aviation, strengthen the presence of Federal Air Marshals aboard U.S.-bound flights, and working with international partners to strengthen international security measures and standards for aviation security.

[20] Details from this section were removed because TSA deemed them Sensitive Security Information, which must be protected from public disclosure pursuant to 49 C.F.R. part 1520.

cost-effectiveness of this acquisition. We analyzed TSA's utilization data collected from March 2010 through February 2011 on all deployed AIT units and found that some deployed units were not used regularly, decreasing their potential security benefit. During this time period, some of the deployed AIT units were used on less than 5 percent of the days they were available since their deployment.[21] Additionally, some units were used on less than 30 percent of the days available since their installation.[22] Moreover, we reported that at some of the 12 airports we visited, AIT units were deployed but were not regularly used. For example, at one airport we observed that TSA had deployed 3 AIT units in an airport terminal that typically handles one flight a day of approximately 230 passengers. TSA officials reported that 2 of the AIT units were seldom used because of the lack of passengers and stated that they believed the AIT units were deployed based on space constraints in areas where they could be placed. According to the Federal Acquisition Regulation, acquisition begins at the point when agency needs are established and includes, among other things, the description of requirements to satisfy agency needs.[23] The limited use of some of these machines may indicate that there was not a clear need for them at the time they were acquired at the locations in which they were deployed. Each AIT unit costs approximately $250,000 to acquire and install. Additionally, each AIT unit is budgeted for five full-time equivalent (FTE) personnel, each of which costs approximately $63,000 per year.[24] Using these figures, we estimate that the first year total cost–including acquisition, installation, and equipment operator salary—was several million dollars.[25] In January 2012, we made a recommendation to TSA to study current AIT utilization and address the extent to which currently

[21] The specific number of AIT units used on less than 5 percent of the days available since their deployment was deleted because it is considered Sensitive Security Information.

[22] The specific number of AIT units used on less than 30 percent of the days available since their installation was deleted because it is considered Sensitive Security Information.

[23] See 48 C.F.R. § 2.101.

[24] We estimated that the 486 AIT units deployed at the time would cost approximately $153 million in labor to operate per year. This was based on 5 FTEs per unit and the average TSO salary and benefit cost of $63,000.

[25] We did not include the specific cost information in the public version of the report as it would identify the number of AIT units in question, which is considered Sensitive Security Information.

deployed AIT units are used. TSA concurred with our recommendation and plans to take efforts to address it.

Additional Actions Needed to Strengthen Internal Controls and Address TWIC Effectiveness

The TWIC program is intended to improve maritime security by using a federally sponsored credential to enhance access controls to secure areas at MTSA-regulated facilities and vessels. As of March 20, 2012, the TWIC program has enrolled over 2.1 million maritime workers and issued nearly 2 million credentials. The TWIC is to be used by individuals requesting unescorted access to MTSA-regulated facilities and vessels and currently is to be visually inspected by facility and vessel operators. The following describes progress made and challenges faced by DHS related to the TWIC program's system of internal controls and DHS's efforts in assessing the effectiveness of TWIC.

Internal Controls. DHS has established a system of TWIC-related processes and controls to assist in implementation of the program. In May 2011, we reported that internal control weaknesses governing the enrollment, background checking, and use of TWIC potentially limit the program's ability to meet the program's stated mission needs or provide reasonable assurance that access to secure areas of MTSA-regulated facilities is restricted to qualified individuals.[26] Key program weaknesses included an inability to provide reasonable assurance that only qualified individuals can acquire TWICs or that once issued a TWIC, TWIC holders have continued to meet eligibility requirements.

As we reported in May 2011, to meet the stated program purpose, TSA's focus in designing the TWIC program was on facilitating the issuance of TWICs to maritime workers. However, TSA did not assess the internal controls in place to determine whether they provided reasonable assurance that the program could meet defined mission needs for limiting access to only qualified individuals.[27] For example, controls that the TWIC

[26] GAO, *Transportation Worker Identification Credential: Internal Control Weaknesses Need to Be Corrected to Help Achieve Security Objectives*, GAO-11-657 (Washington, D.C.: May 10, 2011).

[27] In accordance with GAO, *Standards for Internal Control in the Federal Government,*GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999), the design of the internal controls is to be informed by identified risks the program faces from both internal and external sources, the possible effect of those risks, control activities required to mitigate those risks, and the cost and benefits of mitigating those risks.

program had in place to identify the use of potentially counterfeit identity documents were not used to routinely inform background checking processes. Additionally, controls were not in place to determine whether an applicant has a need for a TWIC. Further, TWIC program controls were not designed to provide reasonable assurance that TWIC holders maintained their eligibility once issued TWICs. For example, controls were not designed to determine whether TWIC holders have committed disqualifying crimes at the federal or state levels after being granted a TWIC.

We further reported that internal control weaknesses in TWIC enrollment, background checking, and use could have contributed to the breach of selected MTSA-regulated facilities during covert tests conducted by our investigators. During these tests at several selected ports, our investigators were successful in accessing port facilities using counterfeit TWICs, authentic TWICs acquired through fraudulent means, and false business cases (i.e., reasons for requesting access). Our investigators did not gain unescorted access to a port where a secondary port-specific identification was required in addition to the TWIC. TSA and Coast Guard officials stated that the TWIC alone is not sufficient and that the cardholder is also required to present a business case. However, our covert tests demonstrated that having an authentic TWIC and a legitimate business case were not always required in practice.

In our May 2011 report, we recommended that the Secretary of Homeland Security perform an internal control assessment of the TWIC program by (1) analyzing existing controls, (2) identifying related weaknesses and risks, and (3) determining cost-effective actions needed to correct or compensate for those weaknesses so that reasonable assurance of meeting TWIC program objectives can be achieved. DHS officials concurred with our recommendations. As of March 2012, DHS reported that it had initiated a review of current internal controls, established a working group with executive oversight to develop and implement solutions to these recommendations, and completed a number of short-term actions to partially address some of the weaknesses. We plan to assess these actions as part of our review of the TWIC pilot and will issue a report on our assessment later this year.

TWIC's Effectiveness. As we reported in May 2011, DHS asserted that the absence of the TWIC program would leave America's critical maritime

port facilities vulnerable to terrorist activities.[28] However, to date, DHS has not assessed the effectiveness of TWIC at enhancing security or reducing risk for MTSA-regulated facilities and vessels. Further, DHS has not demonstrated that TWIC, as currently implemented and planned with card readers, is more effective than prior approaches used to limit access to ports and facilities, such as using facility-specific identity credentials with business cases (i.e., reasons for requesting access).

According to TSA and Coast Guard officials, because the program was mandated by Congress as part of MTSA, DHS did not conduct a risk assessment to identify and mitigate program risks prior to implementation. However, internal control weaknesses raise questions about the effectiveness of the TWIC program. Moreover, as we have previously reported, Congress also needs information on whether and in what respects a program is working well or poorly to support its oversight of agencies and their budgets, and agencies' stakeholders need performance information to accurately judge program effectiveness. Therefore, we recommended in our May 2011 report that the Secretary of Homeland Security conduct an effectiveness assessment that includes addressing internal control weaknesses and, at a minimum, evaluate whether use of TWIC in its present form and planned use with readers would enhance the posture of security beyond efforts already in place given costs and program risks. We further recommended that the internal control and effectiveness assessments be used as the basis for evaluating the costs, benefits, and security risks of the TWIC program prior to requiring the use of TWICs with card readers. DHS concurred with our recommendation. As of March 2012, DHS reports that it is further evaluating the TWIC program using its risk assessment model. This step could help inform DHS of the TWIC program's effectiveness.

Chairmen Issa and Mica, Ranking Members Cummings and Rahall, and Members of the Committees, this concludes my prepared statement. I would be pleased to respond to any questions that you may have at this time.

[28] See DHS, *Transportation Worker Identification Credentialing (TWIC)*, DHS Exhibit 300 Public Release BY10/TSA (Washington, D.C.: Apr. 17, 2009), and *Transportation Worker Identification Credentialing (TWIC)*, DHS Exhibit 300 Public Release BY09/TSA (Washington, D.C.: July 27, 2007).

GAO Contact and Staff Acknowledgments

If you or your staff have any questions about this testimony, please contact me 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. Individuals making key contributions to this testimony are David M. Bruno, Assistant Director; Steve D. Morris, Assistant Director; Carissa Bryant; Joseph P. Cruz; and Emily Gunn. Key contributors to the previous work that this testimony is based on are listed in each individual product.

Stephen Lord - Bio

Steve Lord is the GAO executive responsible for directing GAO's numerous engagements on aviation and surface transportation security issues.

Mr. Lord is a recognized expert on TSA's passenger, checked baggage, and air cargo screening systems and regularly discusses these issues before Congress and industry forums.

Before his appointment to GAO's senior executive service, he led GAO's work on a number of key international security and finance programs.

He holds an undergraduate degree from the University of Virginia, a M.B.A. from George Mason University, a M.S. in national security strategy from the National War College, and completed the Senior Executive Fellows program at Harvard University in May 2008.